Docket No. 1341.1044/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Takayuki HASEBE, et al.	)	Group Art Unit: To Be Assigned
	)	
Serial No.: To Be Assigned	)	Examiner: To Be Assigned
	)	
Filed: April 13, 2000	)	
	)	
For: SIGNATURE CREATING APPARATUS, SIGNATURE VERIFICATION APPARATUS AND SIGNATURE APPARATUS	)	

#3
7-11-00
P.Z.

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 11-151709 filed May 31, 1999.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY, LLP

Dated: April 13, 2000

By: _____
James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
(202) 434-1500

PFJA-000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed h this Office.

出 願 年 月 日
ate of Application: １９９９年　５月３１日

願 番 号
plication Number: 平成１１年特許願第１５１７０９号

願　　人
licant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　２月１８日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号　出証特２０００－３００７３２

【書類名】　特許願

【整理番号】　9950661

【提出日】　平成11年 5月31日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

H04L　9/32

【発明の名称】　署名作成装置および署名検証装置ならびに署名装置

【請求項の数】　16

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　長谷部　高行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　秋山　良太

【発明者】

【住所又は居所】　東京都港区芝浦四丁目１５番３３号　株式会社富士通ビー・エス・シー内

【氏名】　佐々木　孝興

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9717671

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　署名作成装置および署名検証装置ならびに署名装置

【特許請求の範囲】

【請求項１】　ディジタル署名を作成する署名作成装置において、

時刻認証機関によってのみ時刻情報が設定される時計と、

前記時刻情報および作成装置を特定するための装置ＩＤを平文に連結する連結手段と、

前記連結手段により作成された連結データ、および署名作成専用の鍵を用いて前記ディジタル署名を作成する署名作成手段と、

を備えることを特徴とする署名作成装置。

【請求項２】　前記連結手段は、前記時刻情報および前記装置ＩＤに加えて、ディジタル署名を作成した者を特定するための個人特定情報を前記平文に連結することを特徴とする請求項１に記載の署名作成装置。

【請求項３】　前記個人特定情報を記憶する記憶手段と、

前記記憶手段の記憶内容の更新を行う更新者が、正当な権限を有する者であるか否かを判断する判断手段と、

前記判断手段により前記更新者が正当な権限を有する者であると判断された場合にのみ、前記記憶手段の記憶内容を更新する更新手段とを備えることを特徴とする請求項２に記載の署名作成装置。

【請求項４】　前記装置ＩＤは、書き換え不可能な記憶手段に記憶されていることを特徴とする請求項１～３のいずれか一つに記載の署名作成装置。

【請求項５】　前記時計の動作状態を確認する確認手段を備え、前記署名作成手段は、前記確認手段により前記時計が正常に動作していることが確認された場合にのみ、前記ディジタル署名を作成することを特徴とする請求項１～４のいずれか一つに記載の署名作成装置。

【請求項６】　前記署名作成手段は、前記確認手段により前記時計が正常に動作していないと確認された場合、前記署名作成専用の鍵の利用を停止し、前記時刻情報を含まない連結情報と前記署名作成専用の鍵以外の鍵とを用いて、ディジタル署名を作成することを特徴とする請求項５に記載の署名作成装置。

【請求項７】　前記確認手段は、前記時計の駆動電圧としきい値との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする請求項５または６に記載の署名作成装置。

【請求項８】　前記確認手段は、一時点前の前記時計の計時結果と、現時点の計時結果との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする請求項５または６に記載の署名作成装置。

【請求項９】　前記確認手段は、前記時計が正常動作している場合、フラグをオンにし、前記時計が正常動作していない場合、前記フラグをオフにし、

前記署名作成手段は、前記フラグがオンにされている場合にのみ、前記ディジタル署名を作成することを特徴とする請求項５または６に記載の署名作成装置。

【請求項１０】　前記時刻認証機関に設置され、時刻設定要求に応じて、前記時刻情報の設定を行う設定手段を備えることを特徴とする請求項１～９のいずれか一つに記載の署名作成装置。

【請求項１１】　前記時刻認証機関に設置され、前記時計に対して自動的に校正をかける校正手段を備えることを特徴とする請求項１～９のいずれか一つに記載の署名作成装置。

【請求項１２】　共通鍵方式を用いてディジタル署名を作成する署名作成装置であって、

作成装置を特定するための装置ＩＤを平文に連結する連結手段と、

前記連結手段により作成された連結データ、および署名作成専用の共通鍵を用いて前記ディジタル署名を作成する署名作成手段と、

を備えることを特徴とする署名作成装置。

【請求項１３】　時刻認証機関によってのみ時刻情報が設定される時計と、前記時刻情報および作成装置を特定するための装置ＩＤを平文に連結する連結手段と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてディジタル署名を作成する署名作成手段とを備える署名作成装置により作成された前記ディジタル署名に基づいて改竄の検証を行う署名検証装置であって、

前記ディジタル署名が連結された前記平文を受信する受信手段と、

前記ディジタル署名、前記平文、および署名検証専用の鍵を用いて、改竄を検

証する署名検証手段と、

を備えることを特徴とする署名検証装置。

【請求項１４】　鍵認証機関から、前記署名検証専用の鍵が暗号化された暗号情報の提供を受け、該暗号情報を復号することにより前記署名検証専用の鍵を生成する署名検証鍵生成手段を備えることを特徴とする請求項１３に記載の署名検証装置。

【請求項１５】　時刻認証機関によってのみ時刻情報が設定される時計と、

前記時刻情報および作成装置を特定するための装置ＩＤを平文に連結する連結手段と、

前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてディジタル署名を作成する署名作成手段と、

前記ディジタル署名が連結された前記平文を受信する受信手段と、

前記ディジタル署名、前記平文、および署名検証専用の鍵を用いて、改竄を検証する署名検証手段と、

前記作成時に、前記時計、前記連結手段および前記署名作成手段における署名作成機能を有効にし、前記検証時に、前記受信手段および前記署名検証手段における署名検証機能を有効にする機能選択手段と、

を備えることを特徴とする署名装置。

【請求項１６】　下位装置としての機能と上位装置としての機能を切り替える切替手段と、

前記切替手段により上位装置としての機能に切り替えられ、かつ前記機能選択手段により前記署名検証機能が有効にされた場合に、前記下位装置であってかつ前記署名作成機能が有効にされた他の署名装置を特定するための装置ＩＤに基づいて、前記署名検証専用の鍵を生成する鍵生成手段と、

を備え、

前記署名作成専用の鍵と前記署名検証専用の鍵とは、共通鍵方式における共通鍵であり、前記署名検証手段は、前記鍵生成手段により生成された前記署名検証用の鍵を用いて、前記改竄を検証することを特徴とする請求項１５に記載の署名装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子化情報の改竄を防止する署名作成装置および署名検証装置ならびに署名装置に関するものであり、特に、暗号化技術を用いたディジタル署名により署名日時、署名装置、署名者等の認証を行うことで改竄を効果的に防止する署名作成装置および署名検証装置ならびに署名装置に関するものである。

【０００２】

紙ベースで処理されていたドキュメント、帳票等は、ペーパレス化の要請から、徐々に電子化された電子化情報としてコンピュータにより処理されている。この種の電子化情報を扱う場合には、電子化情報を作成した本人になりすました第三者による改竄が行われる可能性がある。そこで、従来より、電子化情報に対する改竄が行われていないことを認証する技術として、暗号化技術を用いたディジタル署名技術が注目されている。特に、現在、飛躍的に普及しているイントラネット、インターネットを介して電子化情報をやりとりする場合に、ディジタル署名技術は、セキュリティを確保するための技術として必須となりつつある。

【０００３】

【従来の技術】

従来より、イントラネットやインターネットを介して電子化情報（以下、平文と称する）を送信する際、平文の内容が改竄されていないことを認証するために、平文を署名鍵を用いて暗号化してディジタル署名を作成した後、このディジタル署名を平文に添付したものを送信している。また、受信側においては、上記ディジタル署名に基づいて、電子化情報が改竄されているか否かを検証している。このような、ディジタル署名の作成／検証には、署名装置が用いられている。

【０００４】

ここで、ディジタル署名の作成／検証には、代表的な暗号化の方式である共通鍵方式または公開鍵方式が採用されている。この共通鍵方式は、作成側（送信側）と検証側（受信側）とで共通の鍵（共通鍵）を保有することに特徴があり、共通鍵方式の代表的なアルゴリズムとしては、周知のＤＥＳ（Data Encryption St

andard）が業界の実質的な標準として用いられている。この共通鍵方式を用いた場合において、作成側の署名装置では、共通鍵を用いて平文を暗号化したものをディジタル署名として作成した後、平文にディジタル署名を添付したものをネットワーク等を介して送信する。

【０００５】

そして、上記ディジタル署名が添付された平文を受信すると、検証側の署名装置では、共通鍵を用いて上記平文を暗号化してディジタル署名を作成した後、このディジタル署名と、受信したディジタル署名とを比較し、この比較結果に基づいて、受信した平文が改竄されているか否かを検証する。すなわち、検証側の署名装置では、両ディジタル署名が一致した場合、平文が改竄されていないことが検証され、両ディジタル署名が一致しない場合、平文が改竄されていることが検証される。

【０００６】

一方、上述した公開鍵方式は、暗号化する鍵と、復号化する鍵とが別々に存在する方式である。一方の鍵は、公開鍵と呼ばれ第三者に対して公開されており、他方の鍵は、プライベート鍵と呼ばれユーザ本人のみが保有している。この公開鍵方式は、公開鍵とプライベート鍵という二つの鍵を利用することで運用を行う方式であるため、公開鍵とプライベート鍵とがなければ暗号化および復号化ができない仕組みになっている。ここで、公開鍵方式の代表的なアルゴリズムとしては、周知のＲＳＡ（Rivest、Shamir、Adleman の３氏の頭文字）が用いられている。

【０００７】

上記公開鍵方式を用いたディジタル署名において、作成者は、自身の公開鍵を第三者に公開するとともに、プライベート鍵を保有している。ここで、作成者の公開鍵が、作成者以外の第三者のいずれもが知り得る鍵であるのに対して、作成者のプライベート鍵は、作成者のみが知りうる鍵である。

【０００８】

上述した公開鍵方式を用いた場合において、作成側の署名装置では、ハッシュ関数により、任意長のビット列からなる平文を固定長のビット列に圧縮（変換）

することでダイジェストを作成する。上記ハッシュ関数は、変換後のダイジェストから変換前の平文を導出することが数学的にほとんど不可能である、という一方向性を有する関数である。そして、作成側の署名装置では、作成者のプライベート鍵を用いて上記ダイジェストを暗号化したものをディジタル署名として作成した後、平文に上記ディジタル署名を添付したものをネットワーク等を介して送信する。

【０００９】

そして、上記ディジタル署名が添付された平文を受信すると、検証側の署名装置では、作成者の公開鍵を用いてディジタル署名を復号し、この復号結果に基づいて、受信した平文が正当な作成者により作成されたものであるか否かを検証する。すなわち、受信したディジタル署名が作成者の公開鍵で復号できた場合、検証側の署名装置では、復号結果としてダイジェストが作成されるとともに、正当な作成側の署名装置（作成者）により、平文が作成されたことが検証される。一方、受信したディジタル署名が作成者の公開鍵で復号できなかった場合、検証側の署名装置では、受信した平文が、正当な作成者になりすました第三者により作成されたことが検証される。

【００１０】

さらに、検証側の署名装置では、作成側の署名装置で用いられたものと同一のハッシュ関数により、受信した平文からダイジェストを作成した後、このダイジェストと、作成者の公開鍵により復号されたダイジェストとを比較することで、送信された平文が改竄されているか否かを検証する。すなわち、検証側の署名装置では、両ダイジェストが一致した場合、平文が改竄されていないことが検証され、両ダイジェストが一致しない場合、平文が改竄されていることが検証される。

【００１１】

ここで、医療用のカルテ、税務帳票、議事録等のドキュメントにおいては、正当な権限を有する作成者が、後日問題が生じた場合に、日時を改竄して新規にドキュメントを作成するという、不正行為に対する防御が必要になる。このような防御にも、前述したディジタル署名技術が応用されている。すなわち、この場合

、には、署名装置の時計より日時情報を得て、これをタイムスタンプとして、上記ドキュメントが電子化された平文に付加したものに対して、ディジタル署名を行うことにより、署名日時が正当であることの認証が可能となる。なお、タイムスタンプを用いた時間認証の詳細については、特開平３－１８５５５１号公報、特開平７－２５４８９７号公報および米国特許第４４５８１０９号公報を参照されたい。

【００１２】

【発明が解決しようとする課題】

ところで、前述したように、従来の署名装置においては、平文にタイムスタンプを付加したものに対してディジタル署名することで署名日時の認証を行っている旨を述べた。しかしながら、作成者により時計の計時結果を容易に変更できるような装置である場合には、作成者が不正利用の目的で、タイムスタンプの内容（日時）を過去の日時に容易に改竄することで、署名日時の正当性が保証されなくなり、ディジタル署名が法的に意味を持たなくなるという問題があった。

【００１３】

また、共通鍵方式を用いた従来の署名装置においては、作成側と検証側とで共通鍵が共に用いられていることから、不正な検証者が正当な作成者に成りすまして、受信した平文に対してディジタル署名を行うことが可能となる。したがって、この場合には、ディジタル署名を行った者の正当性を保証できないという問題が発生する。すなわち、この場合には、ディジタル署名を行った者（装置）を特定することができないという問題が発生する。

【００１４】

さらに、企業組織等においては、ディジタル署名を行った者に関する情報（たとえば、役職名、氏名等）が重要な意味を持つ。このことから、企業組織等においては、職制変更が頻繁に行われるため、かかる変更に柔軟に対応できる署名装置が要請されている。

【００１５】

本発明は、上記に鑑みてなされたもので、日時の改竄を防止することができるとともに、ディジタル署名を行った者、装置を特定することができ、しかも作成

者に関する情報の変更に柔軟に対応できる署名作成装置および署名検証装置ならびに署名装置を提供することを目的とする。

【００１６】

【課題を解決するための手段】

上記目的を達成するために、請求項１にかかる発明は、ディジタル署名を作成する署名作成装置において、時刻認証機関によってのみ時刻情報が設定される時計（後述する実施の形態１および２の時計１０３に相当）と、前記時刻情報および作成装置を特定するための装置ＩＤを平文に連結する連結手段（後述する実施の形態１、２の連結部１０２および連結部１０６に相当）と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いて前記ディジタル署名を作成する署名作成手段（後述する実施の形態１の署名作成回路１１２、実施の形態２の署名作成回路７０２に相当）とを備えることを特徴とする。

【００１７】

この請求項１にかかる発明によれば、時計の時刻情報は、時刻認証機関によってのみ設定されるため、第三者による不正な時刻の改竄が行われることがない。また、請求項１にかかる発明によれば、連結手段により、上記時刻情報および装置ＩＤが平文に連結された後、署名作成手段により、連結データおよび署名作成専用の鍵に基づいてディジタル署名が作成される。このように、請求項１にかかる発明によれば、時計の時刻情報の設定を時刻認証機関以外で行えないようにするとともに、時刻情報および装置ＩＤを含む連結データおよび署名専用の鍵を用いてディジタル署名を作成するようにしたので、日時の改竄を防止することができるとともに、ディジタル署名を作成した装置を特定することができる。

【００１８】

また、請求項２にかかる発明は、請求項１に記載の署名作成装置において、前記連結手段（後述する実施の形態１、２の連結部１０９に相当）は、前記時刻情報および前記装置ＩＤに加えて、ディジタル署名を作成した者を特定するための個人特定情報（たとえば、氏名、職制）を前記平文に連結することを特徴とする。

【００１９】

この請求項２にかかる発明によれば、連結手段により、時刻情報、装置ＩＤに加えて個人特定情報が平文に連結されると、署名作成手段によりディジタル署名が作成される。このように、請求項２にかかる発明によれば、個人特定情報を含む連結データを用いてディジタル署名を作成するようにしたので、検証側でディジタル署名の作成者を容易に特定することができるとともに、作成者に関する情報の変更に柔軟に対応することができる。

【００２０】

また、請求項３にかかる発明は、前記個人特定情報を記憶する記憶手段と、前記記憶手段の記憶内容の更新を行う更新者が、正当な権限を有する者であるか否かを判断する判断手段（後述する実施の形態１、２の時計更新部１０５に相当）と、前記判断手段により前記更新者が正当な権限を有する者であると判断された場合にのみ、前記記憶手段の記憶内容を更新する更新手段（後述する実施の形態１、２の時計更新部１０５に相当）とを備えることを特徴とする。

【００２１】

この請求項３にかかる発明によれば、判断手段により、記憶手段の記憶内容（個人特定情報）を更新する際の更新者が正当な権限を有する者であるか否かが判断され、正当な更新者が正当な権限を有する者であると判断された場合にのみ、更新手段により記憶内容が更新される。このように、請求項３にかかる発明によれば、判断手段を設けたことにより、個人特定情報を不正に更新する第三者を排除することができるため、セキュリティが向上する。

【００２２】

また、請求項４にかかる発明は、請求項１～３のいずれか一つに記載の署名作成装置において、前記装置ＩＤは、書き換え不可能な記憶手段（後述する実施の形態１、２の装置ＩＤ記憶部１０１に相当）に記憶されていることを特徴とする。

【００２３】

この請求項４にかかる発明によれば、装置ＩＤが書き換え不可能な記憶手段（たとえば、ワンタイムＲＯＭ）に記憶されているため、装置ＩＤの改竄を防止することができることから、セキュリティがさらに向上する。

【００２４】

また、請求項５にかかる発明は、請求項１～４のいずれか一つに記載の署名作成装置において、前記時計の動作状態を確認する確認手段（後述する実施の形態１、２のプロセッサに相当）を備え、前記署名作成手段は、前記確認手段により前記時計が正常に動作していることが確認された場合にのみ、前記ディジタル署名を作成することを特徴とする。

【００２５】

この請求項５にかかる発明によれば、確認手段により時計が正常に動作していることが確認された場合にのみ、署名作成手段によりディジタル署名が作成されるようにしたので、時刻情報の信頼性が高水準に維持される。

【００２６】

また、請求項６にかかる発明は、請求項５に記載の署名作成装置において、前記署名作成手段は、前記確認手段により前記時計が正常に動作していないと確認された場合、前記署名作成専用の鍵の利用を停止し、前記時刻情報を含まない連結情報と前記署名作成専用の鍵以外の鍵とを用いて、ディジタル署名を作成することを特徴とする。

【００２７】

この請求項６にかかる発明によれば、時計が故障等に起因して、正常に動作しない場合、すなわち、時刻情報を含む連結データに基づいてディジタル署名が作成できない場合に署名作成専用の鍵の利用を停止し、時刻情報を含まない連結情報と署名作成専用の鍵以外の鍵を用いてディジタル署名を作成できるようにしたので、汎用性が向上する。

【００２８】

また、請求項７にかかる発明は、請求項５または６に記載の署名作成装置において、前記確認手段は、前記時計の駆動電圧としきい値との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする。

【００２９】

この請求項７にかかる発明によれば、確認手段により、駆動電圧としきい値との比較結果において、たとえば、時計の駆動電圧がしきい値電圧より低い場合に

、時計が正常動作していないことを確認するようにしたので、時刻情報の信頼性が高水準に維持される。

【００３０】

また、請求項８にかかる発明は、請求項５または６に記載の署名作成装置において、前記確認手段は、一時点前の前記時計の計時結果と、現時点の計時結果との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする。

【００３１】

この請求項８にかかる発明によれば、確認手段により、一時点前の計時結果と現時点の計時結果との比較結果において、たとえば、両計時結果が一致した場合に、時計が停止していることを確認するようにしたので、時刻情報の信頼性が高水準に維持される。

【００３２】

また、請求項９にかかる発明は、請求項５または６に記載の署名作成装置において、前記確認手段は、前記時計が正常動作している場合、フラグをオンにし、前記時計が正常動作していない場合、前記フラグをオフにし、前記署名作成手段は、前記フラグがオンにされている場合にのみ、前記ディジタル署名を作成することを特徴とする。

【００３３】

この請求項９にかかる発明によれば、確認手段によりフラグがオンにされている場合、すなわち、時計が正常動作している場合にのみ、署名作成手段によりディジタル署名を作成するようにしたので、時刻情報に関して信頼性が高いディジタル署名が作成される。

【００３４】

また、請求項１０にかかる発明は、請求項１～９のいずれか一つに記載の署名作成装置において、前記時刻認証機関に設置され、時刻設定要求に応じて、前記時刻情報の設定を行う設定手段を備えることを特徴とする。

【００３５】

この請求項１０にかかる発明によれば、時刻設定要求に応じて、時刻認証機関に設置された設定手段により時計の時刻設定が行われるようにしたので、第三者

による不正な時刻の改竄が効果的に防止される。

【００３６】

また、請求項１１にかかる発明は、請求項１～９のいずれか一つに記載の署名作成装置において、前記時刻認証機関に設置され、前記時計に対して自動的に校正をかける校正手段を備えることを特徴とする。

【００３７】

この請求項１１にかかる発明によれば、校正手段により自動的に時計が校正されるため、時計から得られる時刻情報の精度が高水準に維持される。

【００３８】

また、請求項１２にかかる発明は、共通鍵方式を用いてディジタル署名を作成する署名作成装置であって、作成装置を特定するための装置ＩＤを平文に連結する連結手段（後述する実施の形態１の連結部１０２に相当）と、前記連結手段により作成された連結データ、および署名作成専用の共通鍵を用いて前記ディジタル署名を作成する署名作成手段（後述する実施の形態１の署名作成回路１１２に相当）とを備えることを特徴とする。

【００３９】

この請求項１２にかかる発明によれば、共通鍵方式において、作成装置を特定するための装置ＩＤを含む連結データおよび署名専用の鍵を用いてディジタル署名を作成するようにしたので、検証側において、ディジタル署名を作成した装置を特定することができる。

【００４０】

また、請求項１３にかかる発明は、時刻認証機関によってのみ時刻情報が設定される時計と、前記時刻情報および作成装置を特定するための装置ＩＤを平文に連結する連結手段と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてディジタル署名を作成する署名作成手段とを備える署名作成装置により作成された前記ディジタル署名に基づいて改竄の検証を行う署名検証装置であって、前記ディジタル署名が連結された前記平文を受信する受信手段（後述する実施の形態１の分離部５０１、実施の形態２の分離部８０１に相当）と、前記ディジタル署名、前記平文、および署名検証専用の鍵を用いて、改竄を検

証する署名検証手段（後述する実施の形態１の署名作成回路５０４および比較部５０５、実施の形態２の圧縮回路８０２、復号回路８０３および比較部８０５に相当）とを備えることを特徴とする。

【００４１】

この請求項１３にかかる発明によれば、受信手段によりディジタル署名が連結された平文が受信されると、署名検証手段は、ディジタル署名、平文および署名検証専用の鍵を用いて、改竄を検証する。このように請求項１３にかかる発明によれば、認証された時刻情報および装置ＩＤを含む連結データに基づいてディジタル署名を検証しているため、日時の改竄を防止することができるとともに、ディジタル署名を作成した装置を特定することができる。

【００４２】

また、請求項１４にかかる発明は、請求項１３に記載の署名検証装置において、鍵認証機関から、前記署名検証専用の鍵が暗号化された暗号情報の提供を受け、該暗号情報を復号することにより前記署名検証専用の鍵を生成する署名検証鍵生成手段を備えることを特徴とする。

【００４３】

この請求項１４にかかる発明によれば、鍵認証機関という信頼性が高い機関より、暗号情報の提供を受け、この暗号情報を署名検証鍵生成手段により復号することで署名検証専用の鍵を生成するようにしたので、装置におけるセキュリティを極めて高くすることができる。

【００４４】

また、請求項１５にかかる発明は、時刻認証機関によってのみ時刻情報が設定される時計（後述する実施の形態３の時計９０３に相当）と、前記時刻情報および作成装置を特定するための装置ＩＤを平文に連結する連結手段（後述する実施の形態３のプロセッサ９０１に相当）と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてディジタル署名を作成する署名作成手段（後述する実施の形態３の署名作成／検証回路９０５に相当）と、前記ディジタル署名が連結された前記平文を受信する受信手段（後述する実施の形態３の入出力バッファメモリ９０２に相当）と、前記ディジタル署名、前記平文、および署

名検証専用の鍵を用いて、改竄を検証する署名検証手段（後述する実施の形態３の署名作成／検証回路９０５に相当）と、前記作成時に、前記時計、前記連結手段および前記署名作成手段における署名作成機能を有効にし、前記検証時に、前記受信手段および前記署名検証手段における署名検証機能を有効にする機能選択手段（後述する実施の形態３のプロセッサ９０１に相当）とを備えることを特徴とする。

【００４５】

この請求項１５にかかる発明によれば、一つの装置に署名作成機能と署名検証機能を持たせることができる。すなわち、請求項１５にかかる発明によれば、機能選択手段により署名作成機能が有効にされると、当該装置が、署名作成装置として機能し、また機能選択手段により署名検証機能が有効にされると、当該装置が、署名検証装置として機能するようにしたので、汎用性を向上させることができる。

【００４６】

また、請求項１６にかかる発明は、請求項１５に記載の署名装置において、下位装置としての機能と上位装置としての機能を切り替える切替手段（後述する実施の形態３のプロセッサ９０１に相当（後述する実施の形態１のプロセッサに相当））と、前記切替手段により上位装置としての機能に切り替えられ、かつ前記機能選択手段により前記署名検証機能が有効にされた場合に、前記下位装置であってかつ前記署名作成機能が有効にされた他の署名装置を特定するための装置ＩＤに基づいて、前記署名検証専用の鍵を生成する鍵生成手段（後述する実施の形態３のプロセッサ９０１に相当（後述する実施の形態１の署名検証鍵生成部５０３に相当））とを備え、前記署名作成専用の鍵と前記署名検証専用の鍵とは、共通鍵方式における共通鍵であり、前記署名検証手段は、前記鍵生成手段により生成された前記署名検証用の鍵を用いて、前記改竄を検証することを特徴とする。

【００４７】

この請求項１６にかかる発明によれば、切替手段により上位装置としての機能に切り替えられ、かつ機能選択手段により署名検証機能が有効にされると、当該署名装置は、署名検証装置として機能する。また、他の署名装置が下位装置とし

ての機能を備え、かつ署名作成装置として機能している状態においてディジタル署名が作成されると、上記署名検証機能を備える上位装置においては、鍵生成手段により下位装置の装置ＩＤに基づい署名検証専用の鍵が生成される。これにより、上位装置の署名検証手段は、上記署名検証専用の鍵を用いて、下位装置からのディジタル署名に基づいて改竄を検証する。このように請求項１６にかかる発明によれば、下位装置が複数台ある場合であっても、上位装置では下位装置の装置ＩＤを管理すればよいため、複数の下位装置のそれぞれの共通鍵を管理する場合のように厳重な管理を行う必要がない。

【００４８】

【発明の実施の形態】

以下、図面を参照して本発明にかかる署名作成装置および署名検証装置ならびに署名装置の実施の形態１～３について詳細に説明する。

【００４９】

（実施の形態１）

図１は、本発明の実施の形態１の構成を示すブロック図である。図１には、前述した共通鍵方式を用いてディジタル署名を作成する署名作成装置１００、および作成されたディジタル署名に基づいて検証を行う署名検証装置５００が図示されている。この図において、署名作成装置１００は、ディジタル署名の作成側に設置されたコンピュータ２００に接続されており、電子化された平文Ａ（図３（ａ）参照）を入力データとして、ディジタル署名を作成する装置である。実際には、署名作成装置１００は、携帯可能なカード型の装置であり、コンピュータ２００のカードスロットに挿入接続されている。この署名作成装置１００の詳細については後述する。

【００５０】

コンピュータ２００は、イントラネット、ローカルエリアネットワーク、インターネット等のネットワーク３００に接続されており、署名作成装置１００からの署名済みデータＭ（図３（ｆ）参照）を送信する機能を備えている。コンピュータ４００は、ディジタル署名の検証側に設置されており、ネットワーク３００に接続されている。このコンピュータ４００は、コンピュータ２００から送信さ

れた署名済みデータＭを受信する機能を備えている。署名検証装置５００は、署名済みデータＭの正当性を検証する装置である。この署名検証装置５００は、署名作成装置１００と同様にして、携帯可能なカード型の装置であり、コンピュータ４００のカードスロットに挿入接続されている。コンピュータ６００は、ＣＡ（Certificate Authority ）センターに設置されており、後述する署名作成装置１００の時計１０３における時刻設定、認証を行う。上記ＣＡセンターは、時刻認証に関してユーザから絶対的な信頼を受けた時刻認証機関である。また、ＣＡセンターは、ディジタル署名、暗号化／復号化に用いられる鍵の認証に関して、ユーザから絶対的な信頼を受けており、公開鍵証明書の発行等を行う鍵認証機関である。

【００５１】

また、作成側の署名作成装置１００の機能としては、下位装置としての機能と、上位装置としての機能とがある。同様にして、検証側の署名検証装置５００の機能としては、下位装置としての機能と、上位装置としての機能とがある。ここで、これらの下位装置と上位装置との関係について図２（ａ）および（ｂ）を参照して説明する。図２（ａ）に示した下位装置１００Ａは、下位装置ＩＤ（Identification number ：識別符号）、署名作成鍵K_{s1}および署名検証鍵K_{c1}を保持している。上記下位装置ＩＤは、下位装置１００Ａを特定するためのＩＤである。署名作成鍵K_{s1}は、ディジタル署名の作成専用の鍵であり、他の目的に利用できないようにインプリメントされている。この署名作成鍵K_{s1}には、作成専用の鍵であることを表す作成属性データS_d が付加されている。署名検証鍵K_{c1}は、ディジタル署名の検証専用の鍵であり、他の目的に利用できないようにインプリメントされている。この署名検証鍵K_{c1}には、検証専用の鍵であることを表す検証属性データC_d が付加されている。

【００５２】

一方、図２（ｂ）に示した上位装置１００Ｂは、上述した作成属性データS_dと同様の作成属性データS_d’が付加された署名作成鍵K_{s1}’、検証属性データC_dと同様の検証属性データC_d’が付加された署名検証鍵K_{c1}’を保持している。また、上位装置１００Ｂは、下位装置ＩＤを用いて署名作成鍵K_{s1}’を署名

検証鍵K_{s1}”に変換する機能を備えている。たとえば、署名検証鍵K_{s1}”は、下位装置ＩＤが署名作成鍵K_{s1}’で暗号化されたものであり、ディジタル署名の検証専用の鍵である。この署名検証鍵K_{s1}”と下位装置１００Ａの署名作成鍵K_{s1}とは、対をなしており、共通鍵方式における共通鍵である。したがって、下位装置１００Ａにおいて署名作成鍵K_{s1}を用いて作成されたディジタル署名は、上位装置１００Ｂにおいて生成された署名検証鍵K_{s1}”によってのみ検証が可能である。

【００５３】

さらに、上位装置１００Ｂは、下位装置ＩＤを用いて署名検証鍵K_{c1}’を署名作成鍵K_{c1}”に変換する機能を備えており、この署名作成鍵K_{c1}”は、下位装置ＩＤが署名検証鍵K_{c1}’で暗号化されたものであり、ディジタル署名の作成専用の鍵である。この署名作成鍵K_{c1}”と下位装置１００Ａの署名検証鍵K_{c1}とは、対をなしており、共通鍵方式における共通鍵である。したがって、上位装置１００Ｂにおいて署名作成鍵K_{c1}”を用いて作成されたディジタル署名は、下位装置１００Ａの署名検証鍵K_{c1}によってのみ検証可能である。

【００５４】

このように、上述した方法を用いることにより、下位装置１００Ａが複数台ある場合であっても、上位装置１００Ｂでは下位装置ＩＤを管理すればよいため、複数の下位装置１００Ａのそれぞれの共通鍵を管理する場合のように厳重な管理を行う必要がない。また、上述した方法を用いることにより、管理共通鍵を一方の共通鍵（署名作成鍵K_{s1}、署名検証鍵K_{s1}”）でディジタル署名の作成が可能な装置を下位装置１００Ａのみとすることができるため、上記一方の共通鍵を用いてディジタル署名を作成した装置の特定が可能となる。同様にして、他方の共通鍵（署名作成鍵K_{c1}”、署名検証鍵K_{c1}）でディジタル署名の作成が可能な装置を上位装置１００Ｂのみとすることができるため、上記他方の共通鍵を用いてディジタル署名を作成した装置の特定が可能となる。

【００５５】

ここで、図１に示した署名作成装置１００は、上述した下位装置１００Ａ（図２（ａ）参照）または上位装置１００Ｂ（図２（ｂ）参照）としての機能を備え

ている。一方、署名検証装置５００は、署名作成装置１００が下位装置１００Ａとしての機能を備えている場合、上位装置１００Ｂとしての機能を備える。この場合とは逆に署名作成装置１００が上位装置１００Ｂとしての機能を備えている場合、署名検証装置５００は、下位装置１００Ａとしての機能を備える。

【００５６】

署名作成装置１００において、装置ＩＤ記憶部１０１は、装置を特定するための装置ＩＤ・Ｂ（図３（ｂ）参照）を記憶する。この装置ＩＤ記憶部１０１は、ワンタイムＲＯＭ（Read Only Memory）等の書き換え不可能な記憶デバイスからなる。したがって、署名作成装置１００においては、装置ＩＤ・Ｂを外部から変更できないようになっている。連結部１０２は、コンピュータ２００から入力される平文Ａ（図３（ａ）参照）と、装置ＩＤ記憶部１０１から読み出された装置ＩＤ・Ｂ（図３（ｂ）参照）とを連結する。

【００５７】

時計１０３は、ディジタル署名の作成の日時の認証に用いられる、日付、時刻等の時間に関する時刻情報を生成する。この時計１０３には、駆動用の電池１０４が内蔵されている。この電池１０４は、一次電池または充電可能な二次電池である。時計更新部１０５は、時計１０３における時刻の更新（設定）時に用いられるものであり、コンピュータ２００およびネットワーク３００を介してコンピュータ６００にアクセスすることで、時刻設定の要求を行う。すなわち、時計１０３は、ＣＡセンターに設置されたコンピュータ６００以外からは、時刻の設定ができないようになっている。また、時計更新部１０５とコンピュータ６００とにおいては、署名作成装置１００のプライベート鍵および公開鍵を用いてディジタル署名の作成、検証が行われる。

【００５８】

連結部１０６は、連結部１０２から出力されるデータ（平文Ａ＋装置ＩＤ・Ｂ）に、時計１０３からの時刻情報をタイムスタンプＣ（図３（ｃ）参照）として連結する。個人特定情報記憶部１０７は、ディジタル署名を作成する者を特定するための個人特定情報Ｄ（図３（ｄ）参照）を記憶する。この個人特定情報Ｄとしては、氏名や職制等が挙げられる。個人特定情報更新部１０８は、外部から入

力される個人特定情報に基づいて、個人特定情報記憶部１０７に記憶されている個人特定情報Ｄを更新（入力、変更）する。この個人特定情報更新部１０８を用いて個人特定情報Ｄを更新（入力、変更）できる者は、正当な権限を有する者に限定されている。したがって、署名作成装置１００においては、たとえば、パスワード入力によるセキュリティ機能により、第三者の不正更新（入力、変更）を防止している。連結部１０９は、連結部１０６から出力されるデータ（平文Ａ＋装置ＩＤ・Ｂ＋タイムスタンプＣ）に個人特定情報Ｄ（図３（ｄ）参照）を連結し、これを署名対象データＥとする。

【００５９】

鍵記憶部１１０は、署名作成装置１００が上位装置１００Ｂ（図２（ｂ）参照）としての機能を備える場合、前述した検証属性データC_d'が付加された署名検証鍵K_{cl}'を記憶する。また、鍵記憶部１１０は、署名作成装置１００が下位装置１００Ａ（図２（ａ）参照）としての機能を備える場合、前述した作成属性データS_dが付加された署名作成鍵K_{sl}を記憶する。署名作成鍵生成部１１１は、署名作成装置１００が上位装置１００Ｂとしての機能を備える場合に用いられ、図２（ｂ）を参照して説明したように、下位装置ＩＤと署名検証鍵K_{cl}'とから署名作成鍵K_{cl}"を生成し、これを署名作成回路１１２へ出力する。なお、署名作成装置１００が下位装置１００Ａとしての機能を備える場合には、署名作成鍵生成部１１１の機能が停止され、同図二点鎖線で示したように署名作成鍵K_{sl}（図２（ａ）参照）が署名作成回路１１２に入力される。

【００６０】

署名作成回路１１２は、共通鍵方式におけるＤＥＳを用いることで、署名対象データＥ（図３（ｄ）参照）を署名作成鍵K_{cl}"（または署名作成鍵K_{sl}）で暗号化し、ＭＡＣ（Message Authentication Code ）と呼ばれる認証子（ディジタル署名）を生成する。この認証子は、署名Ｌ（図３（ｅ）参照）として出力される。ここで、署名作成回路１１２においては、署名作成装置１００が上位装置１００Ｂとしての機能を備えている場合、署名作成鍵K_{cl}"が共通鍵として用いられ、署名作成装置１００が下位装置１００Ａとしての機能を備えている場合、署名作成鍵K_{sl}が共通鍵として用いられる。連結部１１３は、署名対象データＥに

署名Ｌを連結し、これを署名済みデータＭ（図３（ｆ）参照）としてコンピュータ２００へ送出する。コンピュータ２００は、ネットワーク３００を介して上記署名済みデータＭをコンピュータ４００へ送出する。

【００６１】

署名検証装置５００において、分離部５０１は、コンピュータ４００により受信された署名済みデータＭ（図４（ａ）参照）を、図４（ｂ）に示したように署名対象データＥと署名Ｌとに分離する。鍵記憶部５０２は、署名検証装置５００が上位装置１００Ｂ（図２（ｂ）参照）としての機能を備える場合、前述した作成属性データS_d'が付加された署名作成鍵K_{s1}'を記憶する。また、鍵記憶部５０２は、署名検証装置５００が下位装置１００Ａ（図２（ａ）参照）としての機能を備える場合、前述した検証属性データC_dが付加された署名検証鍵K_{c1}を記憶する。署名検証鍵生成部５０３は、署名検証装置５００が上位装置１００Ｂとしての機能を備える場合に用いられ、図２（ｂ）を参照して説明したように、下位装置ＩＤ（この場合、署名作成装置１００の装置ＩＤ・Ｂ）と署名作成鍵K_{s1}'とから署名検証鍵K_{s1}"を生成し、これを署名作成回路５０４へ出力する。なお、署名検証装置５００が下位装置１００Ａとしての機能を備える場合には、署名検証鍵生成部５０３の機能が停止され、同図二点鎖線で示したように署名検証鍵K_{c1}（図２（ａ）参照）が署名作成回路５０４に入力される。

【００６２】

署名作成回路５０４は、署名作成装置１００の署名作成回路１１２と同様の機能を備えており、分離部５０１により分離された署名対象データＥ（図４（ｂ）参照）を署名検証鍵K_{s1}"（または署名検証鍵K_{c1}）で暗号化し、ＭＡＣと呼ばれる認証子（ディジタル署名）を生成する。この認証子は、署名Ｎ（図４（ｃ）参照）として出力される。ここで、署名作成回路５０４においては、署名検証装置５００が上位装置１００Ｂとしての機能を備えている場合には、署名検証鍵K_{s1}"が、下位装置１００Ａとしての機能を備える署名作成装置１００における署名作成鍵K_{s1}との共通鍵として用いられる。また、署名検証装置５００が下位装置１００Ａとしての機能を備えている場合には、署名検証鍵K_{c1}が、上位装置１００Ｂとしての機能を備える署名作成装置１００における署名作成鍵K_{c1}"との

共通鍵として用いられる。

【００６３】

比較部５０５は、分離部５０１により分離された署名Ｌ（図４（ｂ）参照）と、署名作成回路５０４により作成された署名Ｎ（図４（ｃ）参照）とを比較することで、署名対象データＥが改竄されているか否かの検証を行う。すなわち、比較部５０５は、両者が一致した場合、検証結果を改竄無しとし、両者が一致しない場合、検証結果を改竄有りとする。

【００６４】

つぎに、上述した実施の形態１の動作について図５に示したフローチャートを参照しつつ説明する。署名作成装置１００において電源がＯＮにされると、図示しないプロセッサは、図５に示したステップＳＡ１へ進み、時計１０３が使用可能状態にあるか否かを示すフラグをチェックした後、ステップＳＡ２へ進む。このフラグがＯＮである場合には、時計１０３が使用可能な状態（ディジタル署名の作成が可能な状態）にあることを示しており、フラグがＯＦＦである場合には、時計１０３が使用不可能な状態（ディジタル署名の作成が不可能な状態）にあることを示している。

【００６５】

ステップＳＡ２では、プロセッサは、フラグがＯＮであるか否かを判断する。ここで、フラグがＯＦＦである場合、プロセッサは、ディジタル署名の作成が不可能であるものと判断し、ステップＳＡ２の判断結果を「Ｎｏ」として、処理を終了する。一方、ステップＳＡ２の判断結果が「Ｙｅｓ」である場合、プロセッサは、ステップＳＡ３へ進み、電池１０４の電圧をチェックした後、ステップＳＡ４へ進む。

【００６６】

ステップＳＡ４では、プロセッサは、チェックした電圧がしきい値以上であるか否かを判断する。ここで、しきい値は、時計１０３の正常な動作を保証する最低電圧である。ステップＳＡ４の判断結果が「Ｎｏ」である場合、プロセッサは、時計１０３が使用不可能な状態、すなわち、タイムスタンプＣの正常性が保証されない状態にあるものとして、ステップＳＡ８へ進み、フラグをＯＦＦにした

後、処理を終了する。一方、ステップＳＡ４の判断結果が「Ｙｅｓ」である場合、プロセッサは、ステップＳＡ５へ進み、時計１０３が動作しているか否かを確認した後、ステップＳＡ６へ進む。具体的には、プロセッサは、時計１０３の計時結果を取得した後、所定時間経過後に再び計時結果を取得し、両計時結果を比較することにより、時計１０３が動作しているか否かを確認する。

【００６７】

ステップＳＡ６では、プロセッサは、時計１０３が正常に動作しているか否かを、ステップＳＡ５の確認結果に基づいて判断する。すなわち、後に取得した計時結果が、先に取得した計時結果より進んでいる場合には、プロセッサは、時計１０３が正常に動作しているものと判断する。他方、両計時結果が一致している場合には、プロセッサは、時計１０３が停止しているものと判断する。ステップＳＡ６の判断結果が「Ｎｏ」である場合、プロセッサは、ステップＳＡ８へ進み、フラグをＯＦＦにした後、処理を終了する。一方、ステップＳＡ６の判断結果が「Ｙｅｓ」である場合、プロセッサは、ステップＳＡ７へ進み、連結情報付き署名処理を実行する。

【００６８】

ここで、上記連結情報とは、図３（ｄ）に示したように平文Ａに連結された情報（装置ＩＤ・Ｂ、タイムスタンプＣ、個人特定情報Ｄ）をいう。また、以下に説明する連結情報付き署名処理において用いられる鍵（署名作成鍵K_{s1}、署名作成鍵K_{s1}'、署名検証鍵K_{s1}''、署名検証鍵K_{c1}、署名検証鍵K_{c1}'、署名作成鍵K_{c1}''：図２（ａ）および（ｂ）参照）は、連結情報付き署名処理において専用に用いられる鍵である。したがって、これらの鍵は、連結情報が連結されていない平文Ａに対するディジタル署名の作成／検証や、平文Ａのみに関する暗号化／復号化に用いられる鍵とは別のものである。

【００６９】

つぎに、連結情報付き署名処理について詳述する。はじめに、署名作成装置１００が下位装置１００Ａ（図２（ａ）参照）としての機能を備えるとともに、署名検証装置５００が上位装置１００Ｂ（図２（ｂ）参照）としての機能を備える場合について説明する。コンピュータ２００より平文Ａが連結部１０２に入力さ

れると、平文Ａには、連結部１０２、連結部１０６および連結部１０９により図３（ｂ）～図３（ｄ）に示したように、装置ＩＤ・Ｂ、タイムスタンプＣおよび個人特定情報Ｄが順次、連結される。そして、署名作成回路１１２および連結部１１３には、署名対象データＥ（図３（ｄ）参照）がそれぞれ入力される。

【００７０】

これにより、署名作成回路１１２では、図３（ｅ）に示したように署名対象データＥが署名作成鍵K_{s1}により暗号化されることで、署名Ｌが作成され、連結部１１３では、図３（ｆ）に示したように、署名対象データＥに上記署名Ｌが連結されることで、署名済みデータＭが作成される。そして、上記署名済みデータＭは、コンピュータ２００により、ネットワーク３００へ送出されることで、コンピュータ４００に受信された後、署名検証装置５００の分離部５０１に入力される。そして、署名済みデータＭ（図４（ａ）参照）は、図４（ｂ）に示したように、分離部５０１により署名対象データＥと署名Ｌとに分離される。

【００７１】

これにより、署名作成回路５０４では、図４（ｃ）に示したように、分離された署名対象データＥが署名検証鍵生成部５０３により生成された署名検証鍵K_{s1}”により暗号化されることで、署名Ｎが作成される。そして、比較部５０５は、分離された他方の署名Ｌと、署名作成回路５０４により作成された署名Ｎとを比較することで、署名対象データＥが改竄されているか否かの検証を行う。ここで、比較部５０５は、両者が一致した場合、検証結果を改竄無しとし、両者が一致しない場合、検証結果を改竄有りとする。

【００７２】

なお、署名作成装置１００が上位装置１００Ｂ（図２（ｂ）参照）としての機能を備えるとともに、署名検証装置５００が下位装置１００Ａ（図２（ａ）参照）としての機能を備える場合、署名作成装置１００の署名作成回路１１２では、前述した署名作成鍵K_{s1}に代えて、署名作成鍵生成部１１１により生成された署名作成鍵K_{c1}”が用いられる。一方、署名検証装置５００の署名作成回路５０４では、前述した署名検証鍵K_{s1}”に代えて署名検証鍵K_{c1}が用いられる。

【００７３】

さて、前述においては、署名作成装置１００における時計１０３の時刻設定が時刻認証機関であるＣＡセンターのコンピュータ６００によってのみ行い得ることを述べた。以下、時計１０３の時刻設定について図６を参照しつつ説明する。この時刻設定は、電池１０４の交換や、電池１０４の充電が行われることにより、前述したフラグがＯＦＦである場合、署名作成装置１００の時計更新部１０５により実行される。この場合、コンピュータ２００から時刻設定のコマンドが入力されると、図６に示したステップＳＲ１では、署名作成装置１００の時計更新部１０５は、コンピュータ２００およびネットワーク３００を経由してＣＡセンターのコンピュータ６００にアクセスし、時刻設定を要求する。これにより、ステップＳＲ２では、コンピュータ６００は、署名作成装置１００の装置ＩＤを要求する。そして、この要求を受けた時計更新部１０５は、ステップＳＲ３で装置ＩＤをコンピュータ６００へ送出する。

【００７４】

つぎのステップＳＲ４では、コンピュータ６００は、正確な日付け、時刻に関する時刻設定情報を送出する。この際、コンピュータ６００は、上記時刻設定情報を、公開鍵方式における署名作成装置１００のプライベート鍵により暗号化することでディジタル署名を作成し、このディジタル署名を時刻設定情報に連結したものを送出する。そして、ディジタル署名付きの時刻設定情報を受信すると、時計更新部１０５は、公開鍵を用いてディジタル署名を検証する。この検証の結果、改竄が無い場合、ステップＳＲ５では、時計更新部１０５は、上記時刻設定情報に基づいて時計１０３を校正することで、正確な時刻設定を行った後、時刻設定の応答をコンピュータ６００に対して行う。なお、この応答時においては、署名作成装置１００のプライベート鍵を用いてディジタル署名を作成し、これをコンピュータ６００へ送信するようにしてもよい。

【００７５】

そして、上記応答を受け取ったコンピュータ６００は、ステップＳＲ６で、時計更新部１０５に対して、校正後の時計１０３の時刻情報を要求する。この要求を受け取った時計更新部１０５は、ステップＳＲ７において時計１０３の時刻情報をコンピュータ６００へ送出する。この際、時計更新部１０５は、上記時刻情

報を、署名作成装置１００のプライベート鍵により暗号化することでディジタル署名を作成し、このディジタル署名を時刻情報に連結したものを送出する。そして、ディジタル署名付きの時刻情報を受信すると、コンピュータ６００は、公開鍵を用いてディジタル署名を検証する。この検証の結果、改竄が無い場合、ステップＳＲ８では、コンピュータ６００により、時刻設定完了の通知が時計更新部１０５へ出される。これにより、署名作成装置１００において、前述したフラグがＯＦＦからＯＮにされた後、一連の時刻設定が完了する。

【００７６】

なお、上述においては、署名作成装置１００側からの時刻設定要求に応じて、コンピュータ６００が時刻設定を行う場合について説明したが、コンピュータ６００から署名作成装置１００（時計更新部１０５）に定期的にアクセスして、時計１０３を自動的に校正するようにしてもよい。この場合の動作について、図７を参照して詳述する。図７に示したステップＳＱ１では、コンピュータ６００は、ネットワーク３００およびコンピュータ２００を経由して署名作成装置１００の時計更新部１０５にアクセスし、署名作成装置１００の装置ＩＤを要求する。そして、この要求を受けた時計更新部１０５は、ステップＳＱ２で装置ＩＤをコンピュータ６００へ送出する。

【００７７】

つぎのステップＳＱ３では、コンピュータ６００は、時計更新部１０５に対して、現時点における時計１０３の時刻情報を要求する。この要求を受け取った時計更新部１０５は、ステップＳＱ４で時計１０３の時刻情報をコンピュータ６００へ送出する。この際、時計更新部１０５は、上記時刻情報を、プライベート鍵により暗号化することでディジタル署名を作成し、このディジタル署名を時刻情報に連結したものを送出する。そして、ディジタル署名付きの時刻情報を受信すると、コンピュータ６００は、公開鍵を用いてディジタル署名を検証する。この検証の結果、改竄が無い場合、コンピュータ６００は、上記時刻情報の誤差の有無を、正確な時刻情報との比較結果に基づいて検証し、誤差がない場合、いずれの処理も行わない。

【００７８】

ここで、誤差がある場合、ステップＳＱ５では、コンピュータ６００は、正確な日付け、時刻に関する時刻設定情報を送出する。この際、コンピュータ６００は、上記時刻設定情報を、署名作成装置１００のプライベート鍵により暗号化することでディジタル署名を作成し、このディジタル署名を時刻設定情報に連結したものを送出する。そして、ディジタル署名付きの時刻設定情報を受信すると、時計更新部１０５は、公開鍵を用いてディジタル署名を検証する。この検証の結果、改竄が無い場合、ステップＳＱ６では、時計更新部１０５は、上記時刻設定情報に基づいて時計１０３を校正することで、正確な時刻設定を行った後、時刻設定の応答をコンピュータ６００に対して行う。なお、この応答時においては、署名作成装置１００のプライベート鍵を用いてディジタル署名を作成し、これをコンピュータ６００へ送信するようにしてもよい。

【００７９】

そして、応答を受け取ったコンピュータ６００は、ステップＳＱ７において時計更新部１０５に対して校正後の時計１０３の時刻情報を要求する。つぎのステップＳＱ８では、時計更新部１０５は、校正後の時刻情報をコンピュータ６００へ送出する。この際、時計更新部１０５は、上記時刻情報を、プライベート鍵により暗号化することでディジタル署名を作成し、このディジタル署名を時刻情報に連結したものを送出する。そして、ディジタル署名付きの時刻情報を受信すると、コンピュータ６００は、公開鍵を用いてディジタル署名を検証する。この検証の結果、改竄が無い場合、ステップＳＱ９では、コンピュータ６００により、時刻設定完了の通知が時計更新部１０５へ出されることで、一連の時刻情報の自動校正が完了する。以後、コンピュータ６００は、定期的に署名作成装置１００の時計更新部１０５へアクセスすることで、時計１０３を自動的に校正する。このような自動校正が行われることにより、時計１０３の時刻情報（タイムスタンプＣ）の精度が高水準に維持される。

【００８０】

なお、上述した実施の形態１においては、図１に示した署名検証鍵生成部５０３により、署名作成鍵K_{s1}'および下位装置ＩＤ情報から署名検証鍵K_{s1}''を生成する例について説明したが、同図２点鎖線で示したように、ＣＡセンターに設

置されたコンピュータ６００からの暗号情報C_rおよび署名検証装置５００の固有鍵K_rから署名検証鍵K_{sl}”を生成するようにしてもよい。すなわち、この場合、コンピュータ６００においては、署名検証装置５００の固有鍵K_rを用いて、署名検証鍵K_{sl}”を暗号化することで、暗号情報C_rを生成する。

【００８１】

そして、コンピュータ６００から上記暗号情報C_rが送出されると、暗号情報C_rは、ネットワーク３００およびコンピュータ４００を経由して、署名検証鍵生成部５０３に入力される。これにより、署名検証鍵生成部５０３は、暗号情報C_rを固有鍵K_rを用いて復号することで、署名検証鍵K_{sl}”を生成する。以下、上述した動作と同様にして、署名作成回路５０４では、上記署名検証鍵K_{sl}”に基づいて署名Ｎを作成する。このような構成によれば、高度の信頼性を有するＣＡセンターに設置されたコンピュータ６００から暗号情報C_rを受け取り、この暗号情報C_rを復号することで署名検証鍵K_{sl}”を生成するようにしたので、署名検証装置５００におけるセキュリティを極めて高くすることができる。

【００８２】

また、上述した実施の形態１においては、連結情報を構成するものとして、装置ＩＤ・Ｂ、タイムスタンプＣおよび個人特定情報Ｄという３つ情報を例に挙げたがこれに限られるものではない。すなわち、連結情報としては、上記３つの情報のうち、１つの情報のみ、または少なくとも２つの情報の組み合わせであってもよい。たとえば、ここで述べている連結情報の例としては、（ａ）項～（ｄ）項が挙げられる。

（ａ）装置ＩＤ・Ｂおよびタイムスタンプ Ｃからなる連結情報

（ｂ）装置ＩＤ・Ｂのみからなる連結情報

（ｃ）タイムスタンプＣのみからなる連結情報

（ｄ）装置ＩＤ・Ｂおよび個人特定情報Ｄからなる連結情報

【００８３】

上記（ａ）項～（ｄ）項のうち、（ａ）項の連結情報および（ｃ）項の連結情報は、いずれもタイムスタンプＣを含む情報であり、一方、（ｂ）項の連結情報および（ｄ）項の連結情報は、タイムスタンプＣを含まない情報である。このよ

うに（ａ）項～（ｄ）項のそれぞれの連結情報が連結された平文Ａに基づいて、署名を作成する場合には、署名作成回路１１２において、それぞれの連結情報に対応する都合４種類の署名作成用の鍵を用いればよい。これら４種類の鍵は、鍵記憶部１１０に記憶させてもよく、また、署名作成鍵生成部１１１により作成するようにしてもよい。

【００８４】

これに関連して、上述した実施の形態１においては、図５を参照して説明したように、電池１０４の電圧がしきい値より低い場合や、時計１０３が正常動作していない場合のように、時計１０３からのタイムスタンプＣ（時刻情報）を用いることができない場合に、連結情報付き署名処理を実行しない例について説明した。しかしながら、このような場合には、プロセッサの制御により、上述した（ａ）項や（ｃ）項のタイムスタンプＣを含む連結情報用の鍵の利用を停止するとともに、上述した（ｂ）項や（ｄ）項の連結情報のようにタイムスタンプＣを含まない連結情報用の鍵を利用することで、（ｂ）項または（ｄ）項の連結情報に基づいて署名を作成すればよい。

【００８５】

以上説明したように、上述した実施の形態１によれば、時計１０３の時刻情報の設定をＣＡセンターのコンピュータ６００以外で行えないようにするとともに、平文Ａに連結情報（装置ＩＤ・Ｂ、タイムスタンプＣ、個人特定情報Ｄ）を連結したものに対して、ディジタル署名を行うようにし、かつ連結情報付きの署名専用の鍵を用いてディジタル署名を行うようにしたので、日時の改竄を防止することができるとともに、ディジタル署名を行った者、装置を特定することができ、作成者を容易に特定することができる。また、実施の形態１によれば、個人特定情報更新部１０８により個人特定情報Ｄを容易に変更可能としたので、職制変更等にも柔軟に対応できる。

【００８６】

（実施の形態２）

図８は、本発明の実施の形態２の構成を示すブロック図である。この図において、図１の各部に対応する部分にはそれぞれ同一の符号を付けその説明を省略す

る。図８には、実施の形態１における共通鍵方式に代えて、公開鍵方式を用いてディジタル署名を作成する署名作成装置７００、および作成されたディジタル署名に基づいて検証を行う署名検証装置８００が図示されている。署名作成装置７００においては、公開鍵方式によるディジタル署名の作成／検証が行われるため、作成者（署名作成装置７００）のプライベート鍵である署名作成鍵K_{s2}が用いられており、他方、署名検証装置８００においては、作成者（署名作成装置７００）の公開鍵である署名検証鍵K_{c2}が用いられている。ここで、署名作成鍵K_{s2}および署名検証鍵K_{c2}は、実施の形態１の場合と同様にして、連結情報付き署名の作成および検証専用の鍵であり、他の目的には使用できないようになっている。

【００８７】

署名作成装置７００は、署名作成装置１００（図１参照）と同様にしてカード型の装置としてコンピュータ２００のカードスロットに挿入・接続されている。この署名作成装置７００は、平文Ａ（図９（ａ）参照）に連結された連結情報（装置ＩＤ・Ｂ、タイムスタンプＣおよび個人特定情報Ｄ（図９（ｂ）、（ｃ）および（ｄ）参照））に関する署名（ディジタル署名）Ｉ（図９（ｇ）参照）を作成する。ここで、署名作成装置７００においては、図１に示した鍵記憶部１１０、署名作成鍵生成部１１１、署名作成回路１１２および連結部１１３に代えて、圧縮回路７０１、署名作成回路７０２、鍵記憶部７０３および連結部７０４が設けられている。

【００８８】

上記鍵記憶部７０３には、署名作成鍵K_{s2}が記憶されており、圧縮回路７０１は、連結部１０９より入力される署名対象データＥ（図９（ｄ）参照）を前述したハッシュ関数によって圧縮したハッシュ値Ｆ（図９（ｅ）参照）に、ビット列からなるＰａｄ値Ｇ（図９（ｆ）参照）を連結することで、ダイジェストＨを作成する。このダイジェストＨは、固定長のビット列からなる。署名作成回路７０２は、図９（ｇ）に示したように、上記ダイジェストＨを署名作成鍵K_{s2}により暗号化することで、署名（ディジタル署名）Ｉを作成する。連結部７０４は、図９（ｈ）に示したように、連結部１０９からの署名対象データＥと、署名作成回

路７０２により作成された署名Ｉとを連結し、これを署名済みデータＪとしてコンピュータ２００へ送出する。

【００８９】

一方、署名検証装置８００は、署名検証装置５００（図１参照）と同様にして、カード型の装置としてコンピュータ４００のカードスロットに挿入・接続されている。この署名検証装置８００は、コンピュータ４００により受信された署名済みデータＪ（図１０（ａ）参照）に基づいて署名Ｉを検証する装置である。署名検証装置８００において、分離部８０１は、図１０（ｂ）に示したように、署名済みデータＪを署名対象データＥと署名Ｉとに分離する。圧縮回路８０２は、署名作成装置７００の圧縮回路７０１と同様の機能を備えている。

【００９０】

すなわち、圧縮回路８０２は、圧縮回路７０１において用いられたものと同じハッシュ関数を用いて、署名対象データＥを圧縮した結果（ハッシュ値）にＰａｄ値を連結することで、図１０（ｃ）に示したダイジェストＫを作成する。復号回路８０３は、図１０（ｄ）に示したように署名Ｉを、鍵記憶部８０４に記憶された署名検証鍵K_{c2}により復号することで、ダイジェストＨを作成する。比較部８０５は、上記ダイジェストＫとダイジェストＨとを比較することにより、署名対象データＥの改竄の有無を検証する。すなわち比較部８０５は、ダイジェストＫとダイジェストＨとが一致する場合には、検証結果を改竄無しとし、両者が一致しない場合には、検証結果を改竄有りとする。

【００９１】

つぎに、上述した実施の形態２の動作について説明する。ここで、実施の形態２における基本的な動作は、図５に示したステップＳＡ１～ステップＳＡ６およびステップＳＡ８、図６に示したステップＳＲ１～ステップＳＲ８、ならびに図７に示したステップＳＱ１～ステップＳＱ９と同様であるため、これらの説明を省略する。したがって、ここでは、実施の形態２におけるステップＳＡ７の連結情報付き署名処理について説明する。

【００９２】

この連結情報付き署名処理において、コンピュータ２００より平文Ａが署名作

成装置７００の連結部１０２に入力されると、平文Ａには、連結部１０２、連結部１０６および連結部１０９により図９（ｂ）～図９（ｄ）に示したように、装置ＩＤ・Ｂ、タイムスタンプＣおよび個人特定情報Ｄが順次、連結される。そして、圧縮回路７０１および連結部７０４には、署名対象データＥ（図９（ｄ）参照）がそれぞれ入力される。

【００９３】

これにより、圧縮回路７０１では、署名対象データＥがハッシュ関数により圧縮されたハッシュ値Ｆ（図９（ｅ）参照）にＰａｄ値Ｇが連結され、ダイジェストＨ（図９（ｆ）参照）が作成される。署名作成回路７０２では、図９（ｇ）に示したようにダイジェストＨが署名作成鍵K_{s2}により暗号化されることで、署名Ｉが作成され、連結部７０４では、図９（ｈ）に示したように、署名対象データＥに署名Ｉが連結されることで、署名済みデータＪが作成される。そして、この署名済みデータＪは、コンピュータ２００により、ネットワーク３００へ送出されることで、コンピュータ４００に受信された後、署名検証装置８００の分離部８０１に入力される。そして、署名済みデータＪ（図１０（ａ）参照）は、図１０（ｂ）に示したように、分離部８０１により署名対象データＥと署名Ｉとに分離される。

【００９４】

これにより、圧縮回路８０２では、図１０（ｃ）に示したように、ハッシュ関数に基づいて署名対象データＥからダイジェストＫが作成される。一方、復号回路８０３では、図１０（ｄ）に示したように、分離された署名Ｉが署名検証鍵K_{c2}により復号されることで、ダイジェストＨが作成される。比較部８０５は、ダイジェストＫとダイジェストＨとを比較し、両者が一致した場合、検証結果を改竄無しとし、両者が一致しない場合、検証結果を改竄有りとする。

【００９５】

以上説明したように、上述した実施の形態２によれば、前述した実施の形態１と同様にして、日時の改竄を防止することができるとともに、ディジタル署名を行った者、装置を特定することができ、作成者を容易に特定することができる。さらに、実施の形態２によれば、個人特定情報更新部１０８により個人特定情報

Ｄを容易に変更可能としたので、職制変更等にも柔軟に対応できる。

【００９６】

（実施の形態３）

さて、前述した実施の形態１および２では、署名作成装置と署名検証装置とを別々に設けた例について説明したが、署名作成機能および署名検証機能の双方を備える署名装置を、作成側および検証側にそれぞれ設けるようにしてもよい。この場合、作成側の署名装置では、署名作成機能を選択するようにし、検証側の署名装置では、署名検証機能を選択するようにすればよい。以下、この場合を実施の形態３として説明する。

【００９７】

図１１は、本発明の実施の形態３の構成を示すブロック図である。この図において、図１および図８の各部に対応する部分には同一の符号を付ける。この図において、署名装置９００Ａは、署名作成／検証機能に加えて、暗号化／復号化機能を備えており、コンピュータ２００に接続されている。署名装置９００Ａにおいて、署名作成／検証機能は、図１に示した署名作成装置１００および署名検証装置５００、ならびに図８に示した署名作成装置７００および署名検証装置８００と同様の機能である。署名装置９００Ｂは、署名装置９００Ａと同一の機能を備えており、コンピュータ４００に接続されている。ここで、署名装置９００Ａおよび署名装置９００Ｂは、カード型の装置であり、コンピュータ２００およびコンピュータ４００のそれぞれのカードスロットに挿入・接続されている。

【００９８】

ここで、図１２を参照して上述した署名装置９００Ａの構成について説明する。この図において、プロセッサ９０１は、装置各部を制御するものであり、図１に示した時計更新部１０５、個人特定情報更新部１０８、署名作成鍵生成部１１１および署名検証鍵生成部５０３と同様の機能を備えている。このプロセッサ９０１の動作の詳細については、フローチャートを参照して後述する。入出力バッファメモリ９０２は、コンピュータ２００との間で入出力されるデータを一時的に記憶するメモリである。時計９０３は、電池９０４により駆動され、図１に示した時計１０３と同様にして、時刻情報を生成する。この時計９０３は、実施の

形態１および２と同様にして、コンピュータ６００（図１１参照）のみにより時刻設定が可能である。電池９０４は、一次電池または充電可能な二次電池である。

【００９９】

署名作成／検証回路９０５は、前述した実施の形態１または２における共通鍵方式または公開鍵方式を用いた署名作成／検証機能を備えている。具体的には、署名作成／検証回路９０５は、図１に示した署名作成装置１００および署名検証装置５００の機能と、図８に示した署名作成装置７００および署名検証装置８００の機能とを備えている。鍵記憶部９０６は、署名作成／検証回路９０５において用いられる署名作成鍵、署名検証鍵（共通鍵、公開鍵、プライベート鍵）を記憶する。これら署名作成鍵および署名検証鍵は、前述した実施の形態１および２において説明したものと同様の鍵である。

【０１００】

ここで、上記署名作成鍵および署名検証鍵は、前述した連結情報付き署名処理専用の鍵であるが、鍵記憶部９０６には、上記専用の鍵の他に、連結情報が連結されていない平文Ａ（図３（ａ）参照）のみに対して、署名作成／検証を行う処理（以下、平文署名処理と称する）のための鍵が記憶されている。さらに、鍵記憶部９０６には、後述する暗号／復号回路９０９において用いられる暗号鍵、復号鍵を記憶している。つまり、署名装置９００Ａは、連結情報付き署名処理、平文署名処理および暗号／復号処理という三つの処理を行えるようになっている。

【０１０１】

個人特定情報記憶部９０７は、個人特定情報記憶部１０７（図１参照）と同様にして、個人特定情報を記憶する。装置ＩＤ記憶部９０８は、装置ＩＤ記憶部１０１（図１参照）と同様にして、署名装置９００Ａを特定するための装置ＩＤを記憶する。暗号／復号回路９０９は、鍵記憶部９０６に記憶されている暗号鍵／復号鍵により、暗号／復号処理を行う。なお、署名装置９００Ｂの構成は、上述した署名装置９００Ａの構成と同様である。ただし、署名装置９００Ｂにおいて、装置ＩＤ記憶部９０８には、署名装置９００Ｂを特定するための装置ＩＤが記憶されている。

【０１０２】

つぎに、上述した実施の形態３の動作について図１３に示したフローチャートを参照しつつ説明する。この場合、図１１に示した署名装置９００Ａは、署名作成の機能に用いられるものとし、他方の署名装置９００Ｂは、署名検証に用いられるものとする。図１３に示したステップＳＢ１では、署名装置９００Ａのプロセッサ９０１は、コンピュータ２００からのコマンド入力に基づいて、連結情報付き署名処理、平文署名処理、暗号／復号処理のうちいずれかの処理を選択する。この場合、連結情報付き署名処理が選択されたものとすると、プロセッサ９０１は、ステップＳＢ４へ進む。なお、平文署名処理が選択された場合、プロセッサ９０１は、ステップＳＢ３へ進み、署名作成／検証回路９０５を制御することで、コンピュータ２００より入力される平文（図３（ａ）参照）に対して署名作成を行う平文署名処理を実行する。また、暗号／復号処理が選択された場合、プロセッサ９０１は、ステップＳＢ２へ進み、暗号／復号回路９０９を制御することで、暗号／復号処理を実行する。

【０１０３】

ステップＳＢ４では、実施の形態１と同様にして、プロセッサ９０１は、時計９０３が使用可能状態にあるか否かを示すフラグをチェックした後、ステップＳＢ５へ進む。このフラグがＯＮである場合には、時計９０３が使用可能な状態（ディジタル署名の作成が可能な状態）にあることを示しており、フラグがＯＦＦである場合には、時計９０３が使用不可能な状態（ディジタル署名の作成が不可能な状態）にあることを示している。

【０１０４】

ステップＳＢ５では、プロセッサ９０１は、フラグがＯＮであるか否かを判断する。ここで、フラグがＯＦＦである場合、プロセッサ９０１は、ディジタル署名の作成が不可能であるものと判断し、ステップＳＢ５の判断結果を「Ｎｏ」として、処理を終了する。一方、ステップＳＢ５の判断結果が「Ｙｅｓ」である場合、プロセッサ９０１は、ステップＳＢ６へ進み、電池９０４の電圧をチェックした後、ステップＳＢ７へ進む。

【０１０５】

ステップＳＢ７では、プロセッサ９０１は、チェックした電圧がしきい値以上であるか否かを判断し、この判断結果が「Ｎｏ」である場合、ステップＳＢ１１へ進み、フラグをＯＦＦにした後、処理を終了する。一方、ステップＳＢ７の判断結果が「Ｙｅｓ」である場合、プロセッサ９０１は、ステップＳＢ８へ進み、時計９０３が動作しているか否かを確認した後、ステップＳＢ９へ進む。ステップＳＢ９では、プロセッサ９０１は、時計９０３が正常に動作しているか否かを、ステップＳＢ８の確認結果に基づいて判断し、この判断結果が「Ｎｏ」である場合、ステップＳＢ１１へ進み、フラグをＯＦＦにした後、処理を終了する。一方、ステップＳＢ９の判断結果が「Ｙｅｓ」である場合、プロセッサ９０１は、ステップＳＢ１０へ進み、図１４に示した連結情報付き署名処理を実行する。

【０１０６】

図１４に示した連結情報付き署名処理において、ステップＳＣ１では、コンピュータ２００（作成者）は、コマンド入力により、署名装置９００Ａに対して署名処理で用いられる鍵を設定する。この場合、署名装置９００Ａが署名作成機能を有する装置として用いられるため、コンピュータ２００は、署名作成用の鍵を、署名装置９００Ａの署名作成／検証回路９０５および鍵記憶部９０６に設定する。したがって、この場合、上記署名作成／検証回路９０５は、署名作成回路として用いられる。

【０１０７】

つぎのステップＳＣ２では、コンピュータ２００は、署名装置９００Ａに対して署名すべき、データ（平文Ａ（図３（ａ）参照））の入力を開始した後、ステップＳＣ３へ進む。ここで、上記データの量が非常に多い場合には、データを複数分割することで、数回に分けて入力が行われる。ステップＳＣ３では、コンピュータ２００は、上記データの入力が完了したか否かを判断し、この判断結果が「Ｎｏ」である場合、ステップＳＣ２へ戻る。そして、データの入力が完了すると、コンピュータ２００は、ステップＳＣ３の判断結果を「Ｙｅｓ」とし、ステップＳＣ４へ進む。ステップＳＣ４では、コンピュータ２００は、署名装置９００Ａの機能（署名作成機能または署名検証機能）を選択する。

【０１０８】

この場合、署名作成機能が選択されると、ステップＳＣ５では、コンピュータ２００は、署名作成コマンドの入力を行う。この署名作成コマンドが署名装置９００Ａのプロセッサ９０１に入力されると、プロセッサ９０１は、上述した実施の形態１（または実施の形態２）における署名作成装置１００（または署名作成装置７００）と同様にして、連結情報付き署名の作成処理を実行する。これにより、図１１に示した署名装置９００Ａからは、署名済みデータＭ（図３（ｆ）参照）（または、署名済みデータＪ（図９（ｈ）参照））がネットワーク３００を介して、コンピュータ４００へ送出される。

【０１０９】

そして、上記署名済みデータＭ（または署名済みデータＪ）を受信すると、コンピュータ４００は、図１４に示したステップＳＣ１では、鍵を設定する。この場合、署名装置９００Ｂが署名検証機能を有する装置として用いられるため、コンピュータ４００は、署名検証用の鍵を、署名装置９００Ｂの署名作成／検証回路９０５および鍵記憶部９０６に設定する。したがって、この場合、署名作成／検証回路９０５は、署名検証回路として用いられる。

【０１１０】

つぎのステップＳＣ２では、コンピュータ４００は、署名装置９００Ｂに対して検証すべき、データ（署名済みデータＭまたは署名済みデータＪ）の入力を開始した後、ステップＳＣ３へ進む。ステップＳＣ３では、コンピュータ４００は、上記データの入力が完了したか否かを判断し、この判断結果が「Ｎｏ」である場合、ステップＳＣ２へ戻る。そして、データの入力が完了すると、コンピュータ４００は、ステップＳＣ３の判断結果を「Ｙｅｓ」とし、ステップＳＣ４へ進む。ステップＳＣ４では、コンピュータ４００は、署名装置９００Ｂの機能（署名作成機能または署名検証機能）を選択する。この場合、署名検証機能が選択されると、ステップＳＣ５では、コンピュータ４００は、署名検証コマンドの入力を行う。

【０１１１】

署名検証コマンドが署名装置９００Ｂのプロセッサ９０１に入力されると、プロセッサ９０１は、上述した実施の形態１（または実施の形態２）における署名

検証装置５００（または署名検証装置８００）と同様にして、連結情報付き署名の検証処理を実行する。なお、署名装置９００Ｂにおいては、図１３に示したステップＳＢ３では、署名装置９００Ａにおいて平文署名が行われたデータに対する検証が行われ、ステップＳＢ２では、署名装置９００Ａにおいて暗号化されたデータに対する復号が行われる。

【０１１２】

以上説明したように、上述した実施の形態３によれば、署名装置９００Ａおよび署名装置９００Ｂに、連結情報付き署名処理、平文署名処理および暗号／復号処理という三つの処理のうち、いずれかの処理を選択して実行するようにしたので、汎用性が向上する。特に、実施の形態３においては、時計９０３が故障したときに、連結情報付き署名処理に代えて平文署名処理を行うことができる。また、上述した実施の形態３によれば、コンピュータ２００およびコンピュータ４００からのコマンド（署名作成コマンド、署名検証コマンド）入力により、署名装置９００Ａおよび署名装置９００Ｂの機能を選択できるようにしたので、汎用性を向上させることができるとともに、インタフェースで共通部分（図１４参照）があるため、実施の形態１、２の場合に比してファームウェアのサイズを小さくすることができる。

【０１１３】

以上本発明の実施の形態１～３について図面を参照して詳述してきたが、具体的な構成例はこの実施の形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。たとえば、実施の形態１においては、図１に示したように、作成側の署名作成装置１００が１台、検証側の署名検証装置５００が１台という１：１の構成例について説明したが、作成側の署名作成装置１００がｎ台に対して、検証側の署名検証装置５００を１台というｎ：１の構成としてもよい。

【０１１４】

このような構成の場合には、ｎ台の署名作成装置１００において、それぞれユニークな共通鍵（署名作成鍵）、または一つの共通鍵（署名作成鍵）を共有して用いる場合が考えられる。作成側でユニークな共通鍵を用いた場合には、署名検

証装置５００においてｎ個の共通鍵（署名検証鍵）を使い分ける必要があるが、セキュリティが向上する。一方、作成側で一つの共通鍵（署名作成鍵）を共有した場合には、署名検証装置５００において一つの共通鍵（署名検証鍵）を用いればよいため、鍵管理が容易となる。

【０１１５】

また、実施の形態１においては、図６および図７を参照して説明したように、署名作成装置１００とコンピュータ６００との間で時刻設定に関する情報の送信／受信に際して、公開鍵方式を用いたディジタル署名を行う例について説明したが、共通鍵方式を用いたディジタル署名を行うようにしてもよい。この時刻設定に関して、署名作成装置１００がｎ台ある場合には、装置毎に異なるプライベート鍵（または共通鍵）を用いるようにすればよい。なお、この場合には、装置間で共通なプライベート鍵（または共通鍵）を共有するようにしてもよい。

【０１１６】

また、実施の形態３において、同一の装置（署名装置９００Ａ）により署名作成／検証を行うようにしてもよい。この場合には、署名装置９００Ａのプロセッサ９０１により検証結果を出す前に、署名済みデータＭ（または署名済みデータＪ）から得られる装置ＩＤと、署名装置９００Ａの装置ＩＤ記憶部９０８に記憶されている装置ＩＤとを比較し、この比較結果が一致した場合にのみ、署名済みデータＭ（または署名済みデータＪ）に対する検証を行うようにしてもよい。なお、上記比較結果が不一致である場合には、署名済みデータＭ（または署名済みデータＪ）が署名装置９００Ａ以外の装置により作成されたことを意味している。最後に、実施の形態１～３のうちいずれか二つまたは三つ組み合わせた構成も、本発明に含まれる。

【０１１７】

【発明の効果】

以上説明したように、請求項１にかかる発明によれば、時計の時刻情報の設定を時刻認証機関以外で行えないようにするとともに、時刻情報および装置ＩＤを含む連結データおよび署名専用の鍵を用いてディジタル署名を作成するようにしたので、日時の改竄を防止することができるとともに、ディジタル署名を作成し

た装置を特定することができるという効果を奏する。

【０１１８】

また、請求項２にかかる発明によれば、個人特定情報を含む連結データを用いてディジタル署名を作成するようにしたので、検証側でディジタル署名の作成者を容易に特定することができるとともに、作成者に関する情報の変更に柔軟に対応することができるという効果を奏する。

【０１１９】

また、請求項３にかかる発明によれば、判断手段を設けたことにより、個人特定情報を不正に更新する第三者を排除することができるため、セキュリティが向上するという効果を奏する。

【０１２０】

また、請求項４にかかる発明によれば、装置ＩＤが書き換え不可能な記憶手段（たとえば、ワンタイムＲＯＭ）に記憶されているため、装置ＩＤの改竄を防止することができることから、セキュリティがさらに向上するという効果を奏する。

【０１２１】

また、請求項５にかかる発明によれば、確認手段により時計が正常に動作していることが確認された場合にのみ、署名作成手段によりディジタル署名が作成されるようにしたので、時刻情報の信頼性が高水準に維持されるという効果を奏する。

【０１２２】

また、請求項６にかかる発明によれば、時計が故障等に起因して、正常に動作しない場合、すなわち、時刻情報を含む連結データに基づいてディジタル署名が作成できない場合に署名作成専用の鍵の利用を停止し、時刻情報を含まない連結情報と署名作成専用の鍵以外の鍵を用いてディジタル署名を作成できるようにしたので、汎用性が向上するという効果を奏する。

【０１２３】

また、請求項７にかかる発明によれば、確認手段により、駆動電圧としきい値との比較結果において、たとえば、時計の駆動電圧がしきい値電圧より低い場合

に、時計が正常動作していないことを確認するようにしたので、時刻情報の信頼性が高水準に維持されるという効果を奏する。

【０１２４】

また、請求項８にかかる発明によれば、確認手段により、一時点前の計時結果と現時点の計時結果との比較結果において、たとえば、両計時結果が一致した場合に、時計が停止していることを確認するようにしたので、時刻情報の信頼性が高水準に維持されるという効果を奏する。

【０１２５】

また、請求項９にかかる発明によれば、確認手段によりフラグがオンにされている場合、すなわち、時計が正常動作している場合にのみ、署名作成手段によりディジタル署名を作成するようにしたので、時刻情報に関して信頼性が高いディジタル署名が作成されるという効果を奏する。

【０１２６】

また、請求項１０にかかる発明によれば、時刻設定要求に応じて、時刻認証機関に設置された設定手段により時計の時刻設定が行われるようにしたので、第三者による不正な時刻の改竄を効果的に防止することができるという効果を奏する。

【０１２７】

また、請求項１１にかかる発明によれば、校正手段により自動的に時計が校正されるため、時計から得られる時刻情報の精度が高水準に維持されるという効果を奏する。

【０１２８】

また、請求項１２にかかる発明によれば、共通鍵方式において、作成装置を特定するための装置ＩＤを含む連結データおよび署名専用の鍵を用いてディジタル署名を作成するようにしたので、検証側において、ディジタル署名を作成した装置を特定することができるという効果を奏する。

【０１２９】

また、請求項１３にかかる発明によれば、認証された時刻情報および装置ＩＤを含む連結データに基づいてディジタル署名を検証しているため、日時の改竄を

防止することができるとともに、ディジタル署名を作成した装置を特定することができるという効果を奏する。

【０１３０】

また、請求項１４にかかる発明によれば、鍵認証機関という信頼性が高い機関より、暗号情報の提供を受け、この暗号情報を署名検証鍵生成手段により復号することで署名検証専用の鍵を生成するようにしたので、装置におけるセキュリティを極めて高くすることができるという効果を奏する。

【０１３１】

また、請求項１５にかかる発明によれば、機能選択手段により署名作成機能が有効にされると、当該装置が、署名作成装置として機能し、また機能選択手段により署名検証機能が有効にされると、当該装置が、署名検証装置として機能するようにしたので、汎用性を向上させることができるという効果を奏する。

【０１３２】

また、請求項１６にかかる発明によれば、下位装置が複数台ある場合であっても、上位装置では下位装置の装置ＩＤを管理すればよいため、複数の下位装置のそれぞれの共通鍵を管理する場合のように厳重な管理を行う必要がないという効果を奏する。

【図面の簡単な説明】

【図１】

本発明にかかる実施の形態１の構成を示すブロック図である。

【図２】

同実施の形態１における下位装置１００Ａと上位装置１００Ｂとの関係を説明する図である。

【図３】

同実施の形態１におけるデータ遷移を示す図である。

【図４】

同実施の形態１におけるデータ遷移を示す図である。

【図５】

同実施の形態１の動作を説明するフローチャートである。

【図６】

同実施の形態１における時刻設定シーケンスを示す図である。

【図７】

同実施の形態１における時刻設定シーケンスを示す図である。

【図８】

本発明にかかる実施の形態２の構成を示すブロック図である。

【図９】

同実施の形態２におけるデータ遷移を示す図である。

【図１０】

同実施の形態２におけるデータ遷移を示す図である。

【図１１】

本発明にかかる実施の形態３の構成を示すブロック図である。

【図１２】

図１１に示した署名装置９００Ａ（９００Ｂ）の構成を示すブロック図である。

【図１３】

同実施の形態３の動作を説明するフローチャートである。

【図１４】

同実施の形態３における連結情報付き署名処理を説明するフローチャートである。

【符号の説明】

１００　署名作成装置

１０１　装置ＩＤ記憶部

１０２　連結部

１０３　時計

１０５　時計更新部

１０６　連結部

１０７　個人特定情報記憶部

１０８　個人特定情報更新部

１０９　連結部

１１１　署名作成鍵生成部

１１２　署名作成回路

２００　コンピュータ

４００　コンピュータ

５００　署名検証装置

５０３　署名検証鍵生成部

５０４　署名作成回路

５０５　比較部

６００　コンピュータ

１００Ａ　下位装置

１００Ｂ　上位装置

７００　署名作成装置

７０２　署名作成回路

８００　署名検証装置

８０３　復号回路

８０５　比較部

９００Ａ　署名装置

９００Ｂ　署名装置

９０１　プロセッサ

９０３　時計

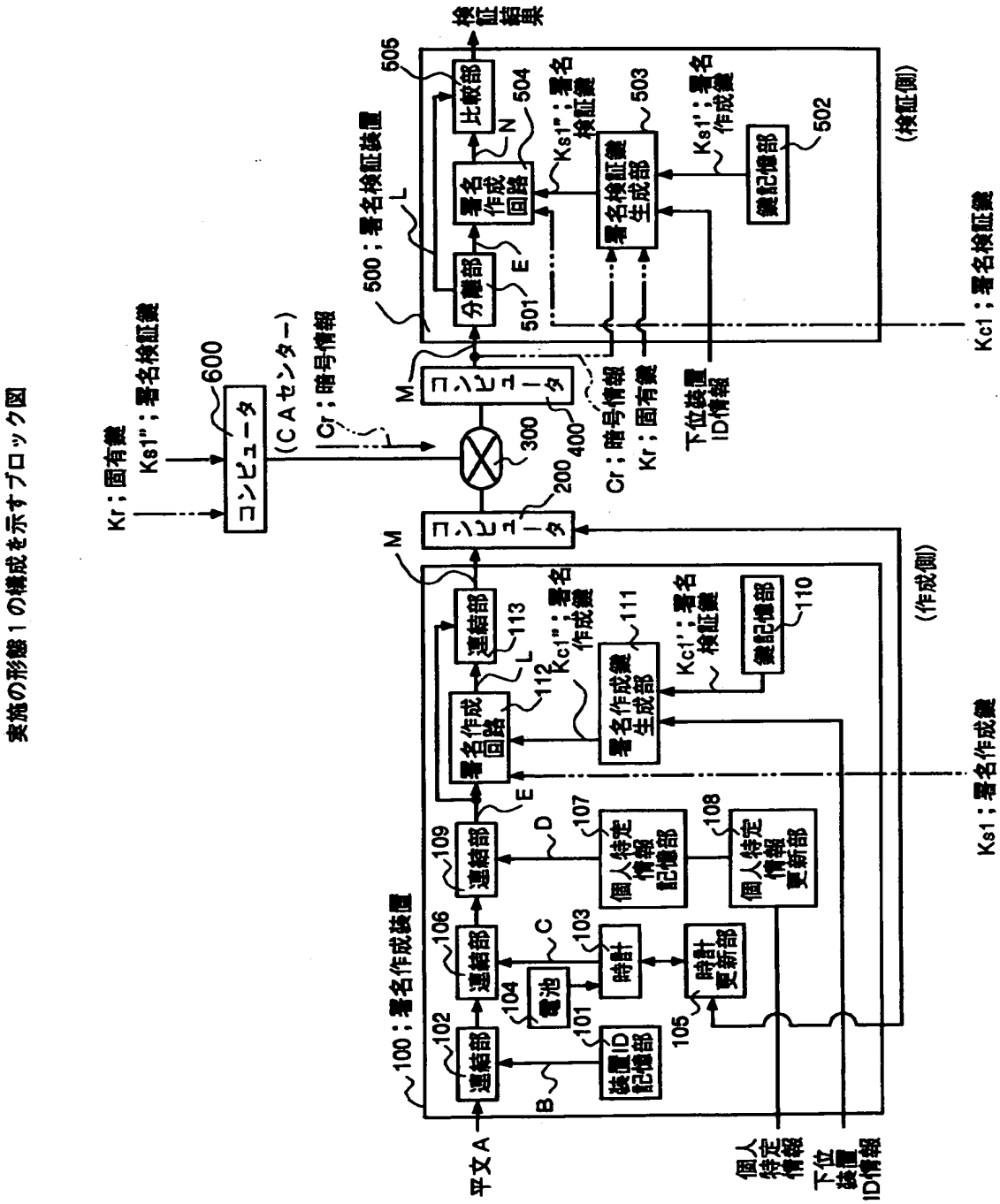
９０５　署名作成／検証回路

９０７　個人特定情報記憶部

９０８　装置ＩＤ記憶部

【書類名】　　図面

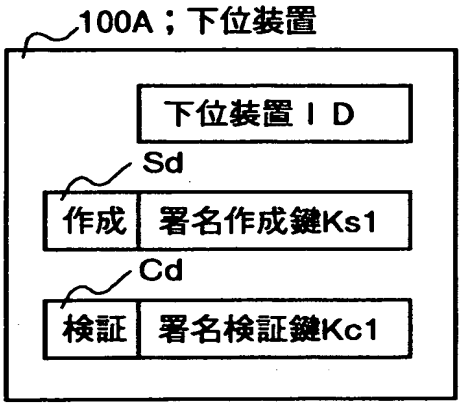
【図１】


実施の形態１の構成を示すブロック図
検証結果
505
比較部
504
署名作成回路
503
署名検証鍵生成部
502
鍵記憶部
分離部
501
500；署名検証装置
（検証側）
Kc1；署名検証鍵
Ks1'；署名作成鍵
Ks1"；署名検証鍵
N
L
E
M
コンピュータ
300
400
200
Cr；暗号情報
Kr；固有鍵
下位装置ID情報
600
コンピュータ
（ＣＡセンター）
Ks1"；署名検証鍵
Kr；固有鍵
Cr；暗号情報
100；署名作成装置
（作成側）
Ks1；署名作成鍵
Kc1"；署名作成鍵
Kc1'；署名検証鍵
113
112
111
110
107
108
109
106
103
104
101
102
105
連結部
署名作成回路
署名作成鍵生成部
鍵記憶部
個人特定情報記憶部
個人特定情報更新部
時計
電池
装置ID記憶部
時計更新部
D
C
B
平文Ａ
個人特定情報
下位装置ID情報

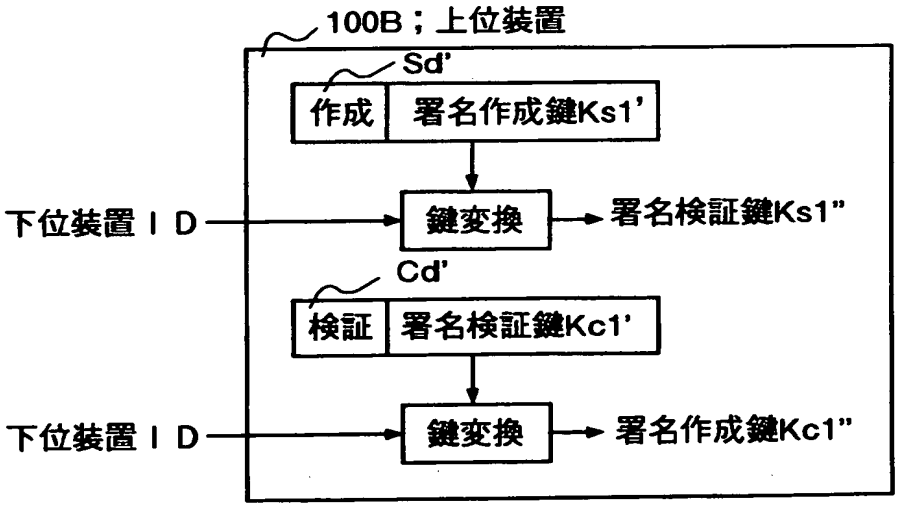
【図２】

実施の形態１における下位装置100Ａと上位装置100Ｂとの関係を説明する図

(a)

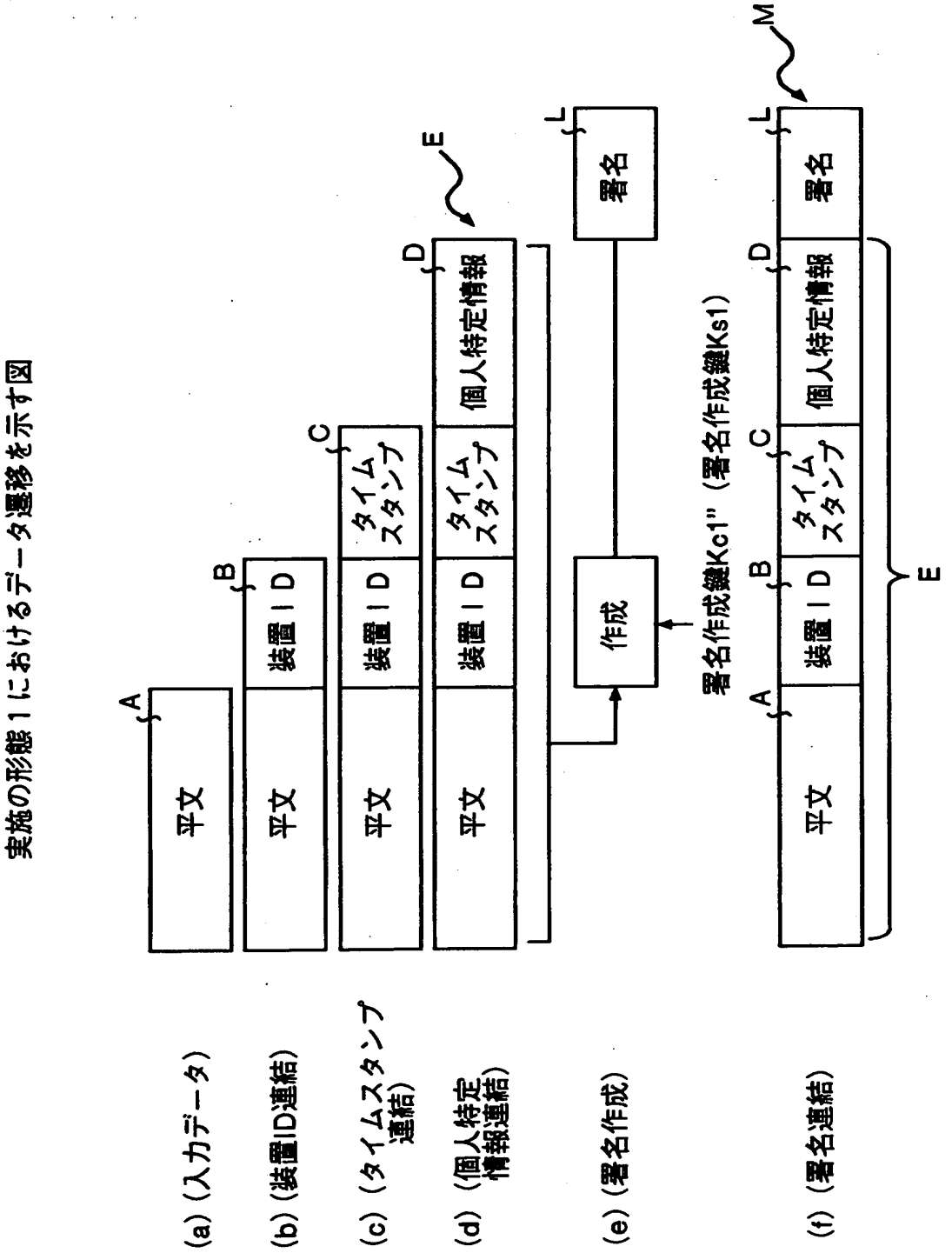


(b)



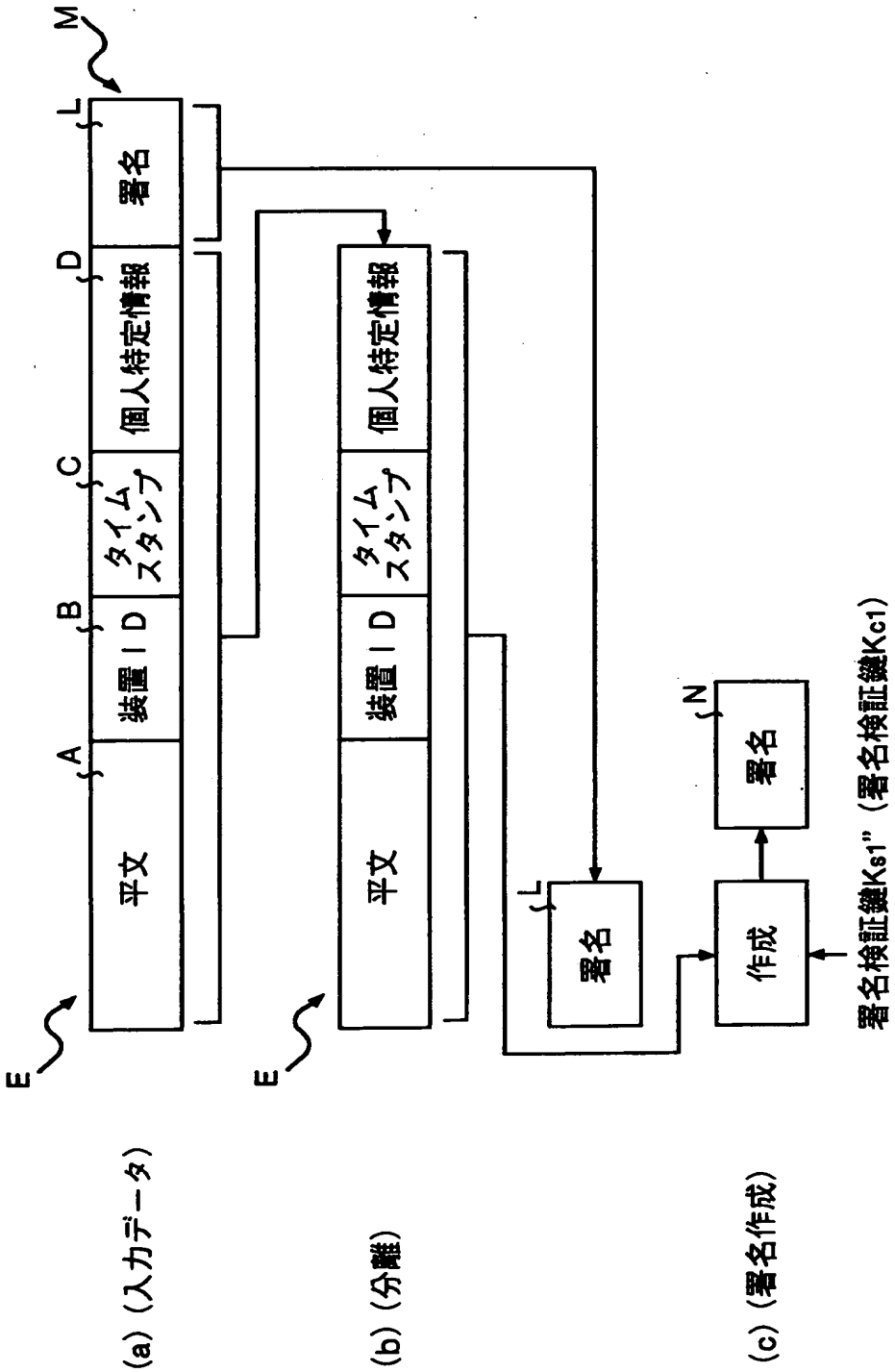
【図３】

実施の形態１におけるデータ遷移を示す図



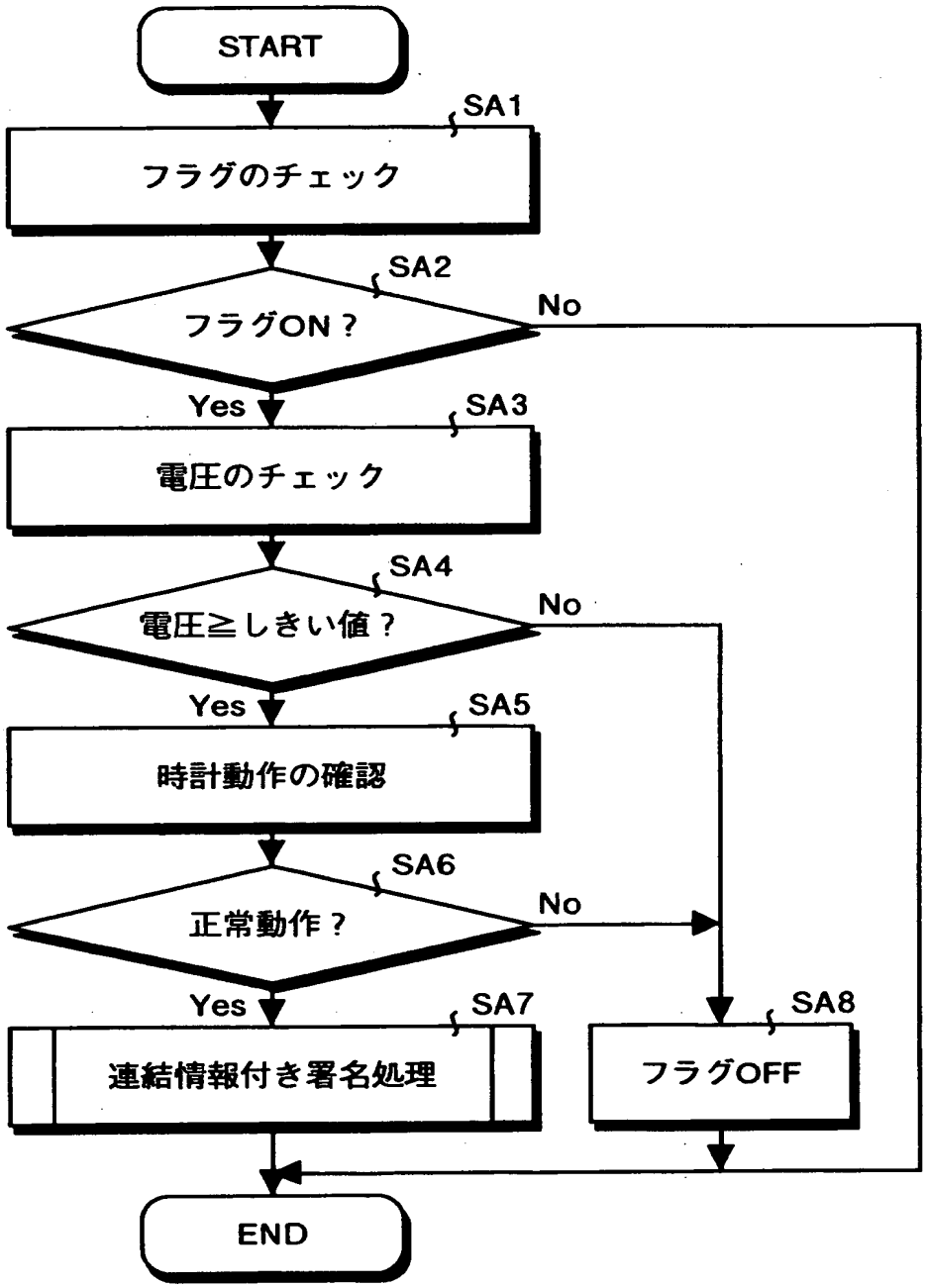
【図４】

実施の形態１におけるデータ遷移を示す図



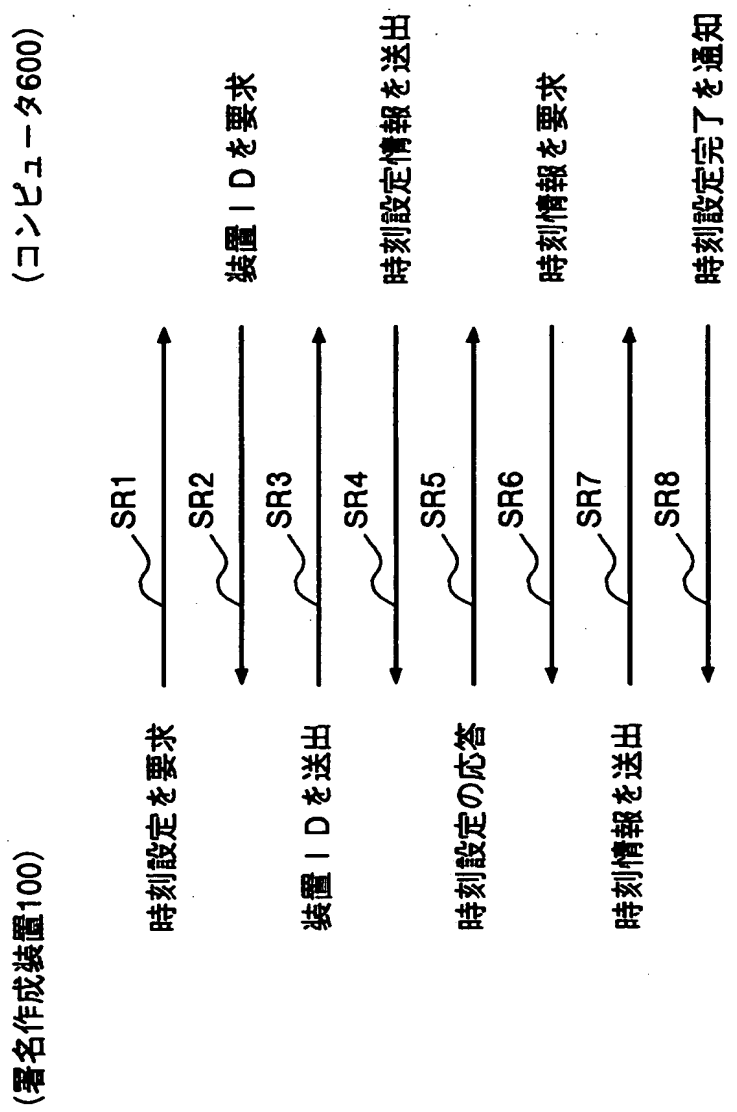
【図５】

実施の形態１の動作を説明するフローチャート



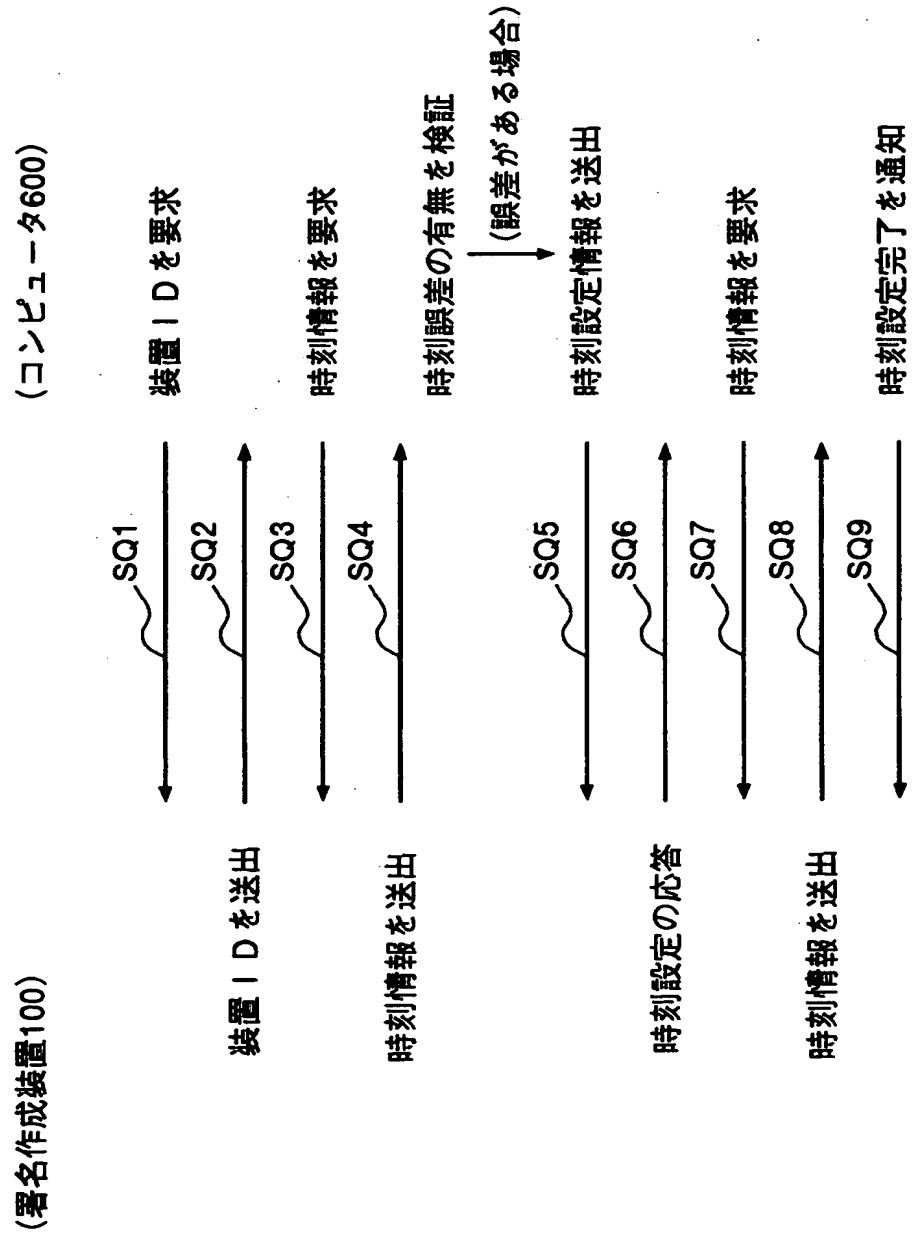
【図６】

実施の形態１における時刻設定のシーケンスを示す図

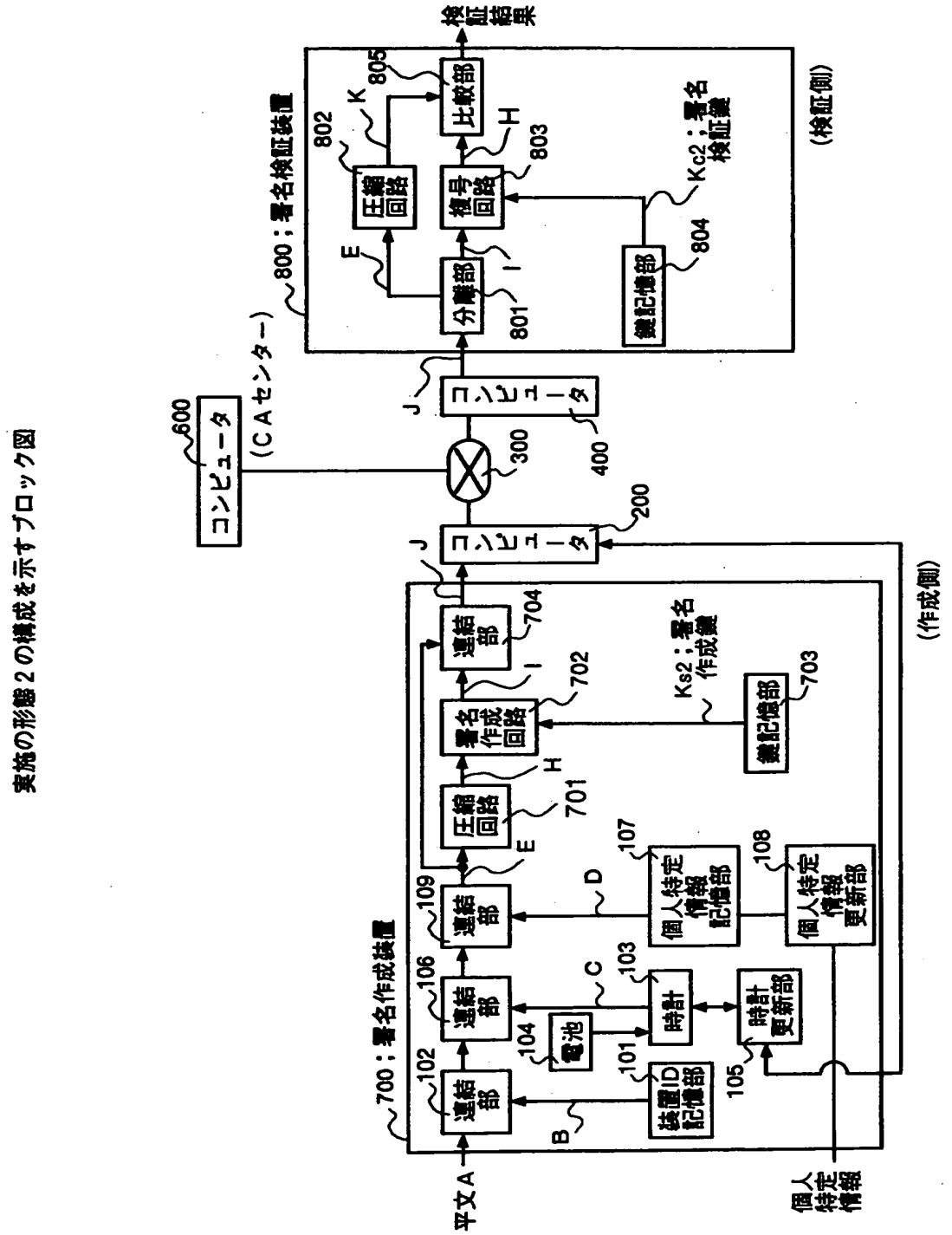


【図７】

実施の形態１における時刻設定シーケンスを示す図

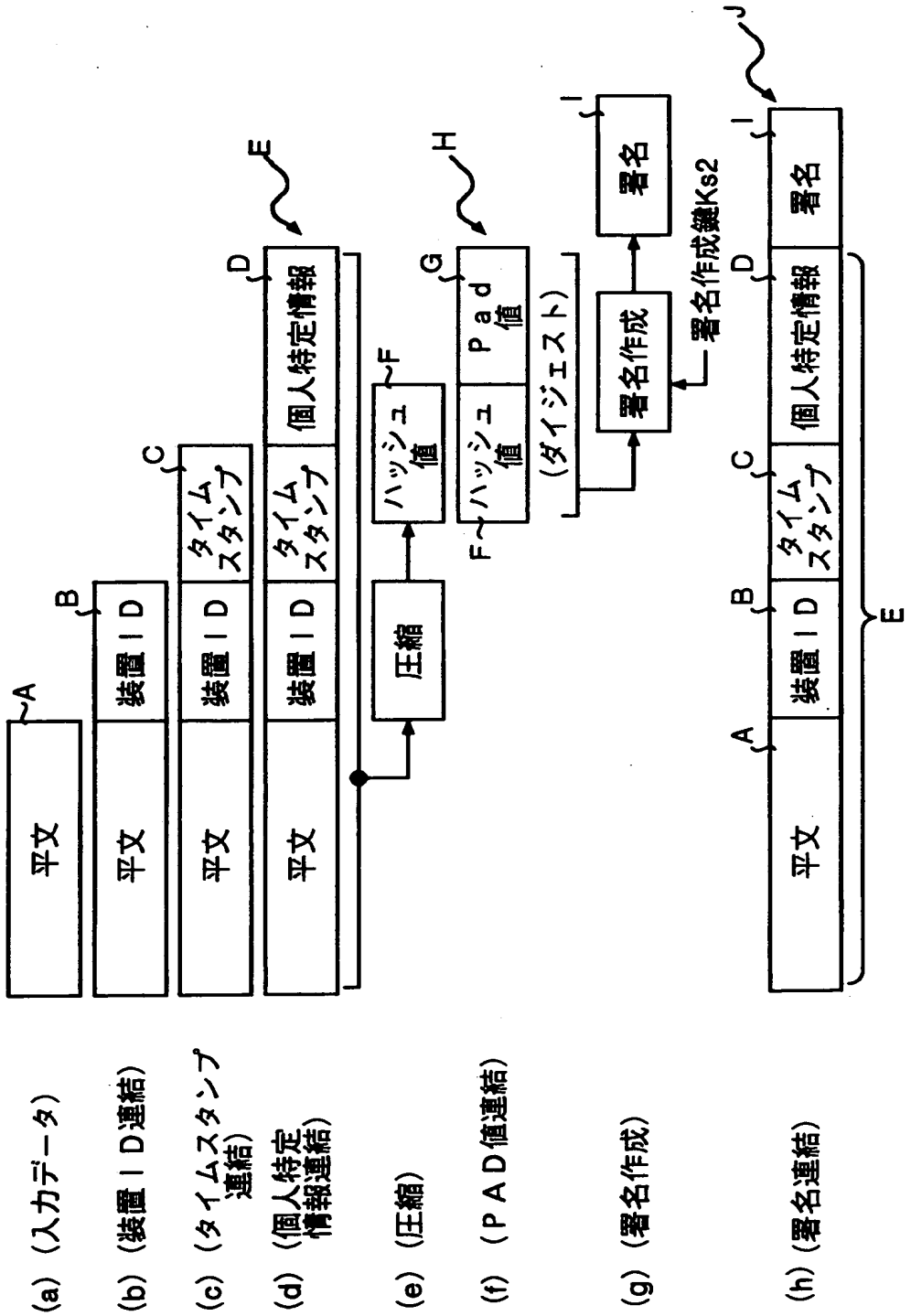


【図８】


実施の形態２の構成を示すブロック図
検証結果
800；署名検証装置
802
K
805
比較部
H
803
圧縮回路
復号回路
Kc2；署名検証鍵
(検証側)
E
I
804
分離部
801
蓄記憶部
J
コンピュータ
600
コンピュータ
(CAセンター)
300
400
200
J
704
連結部
I
702
署名作成回路
Ks2；署名作成鍵
703
蓄記憶部
H
701
圧縮回路
E
107
108
D
109
連結部
個人特定情報記憶部
個人特定情報更新部
700；署名作成装置
106
連結部
C
103
時計
時計更新部
104
電池
102
連結部
101
装置ID記憶部
105
B
平文A
個人特定情報
(作成側)

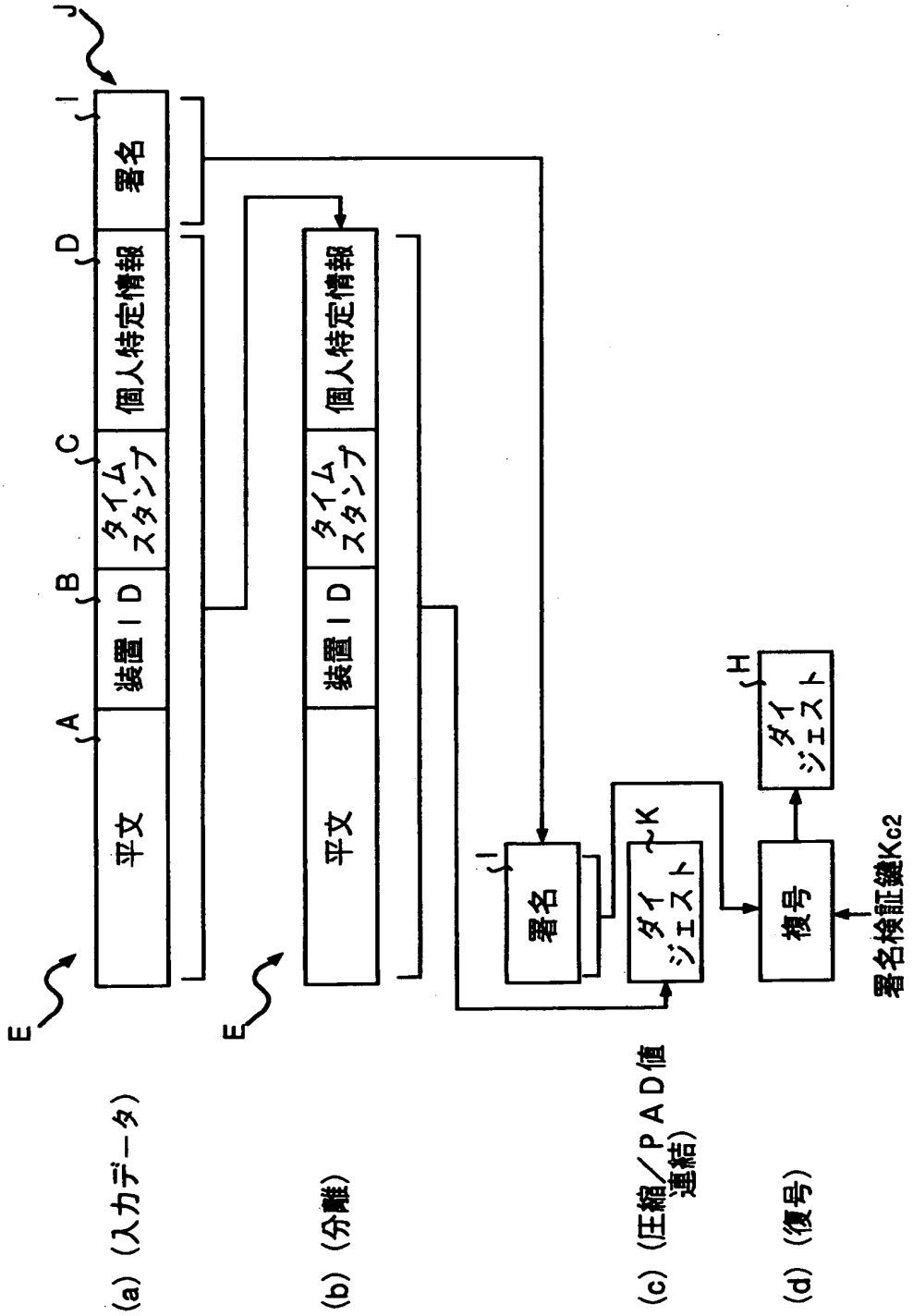
【図９】

実施の形態２におけるデータ遷移を示す図



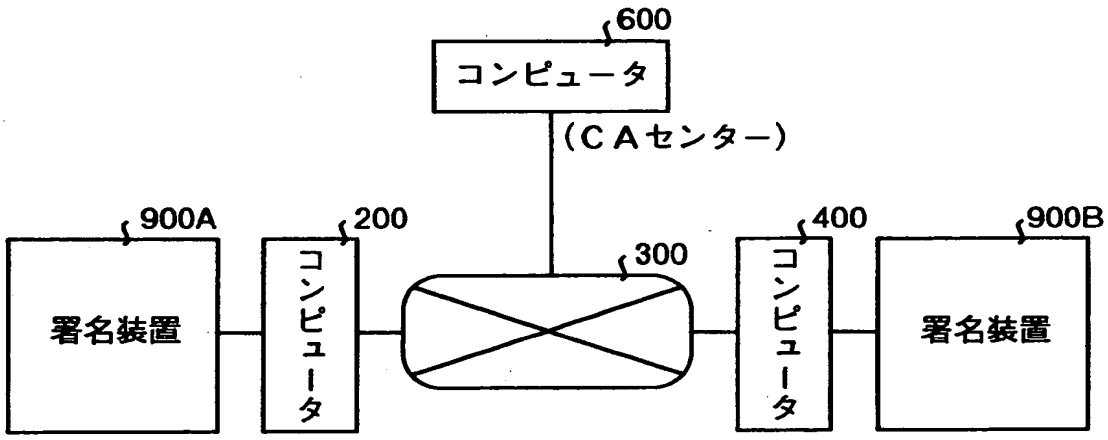
【図１０】

実施の形態２における データ遷移を示す図



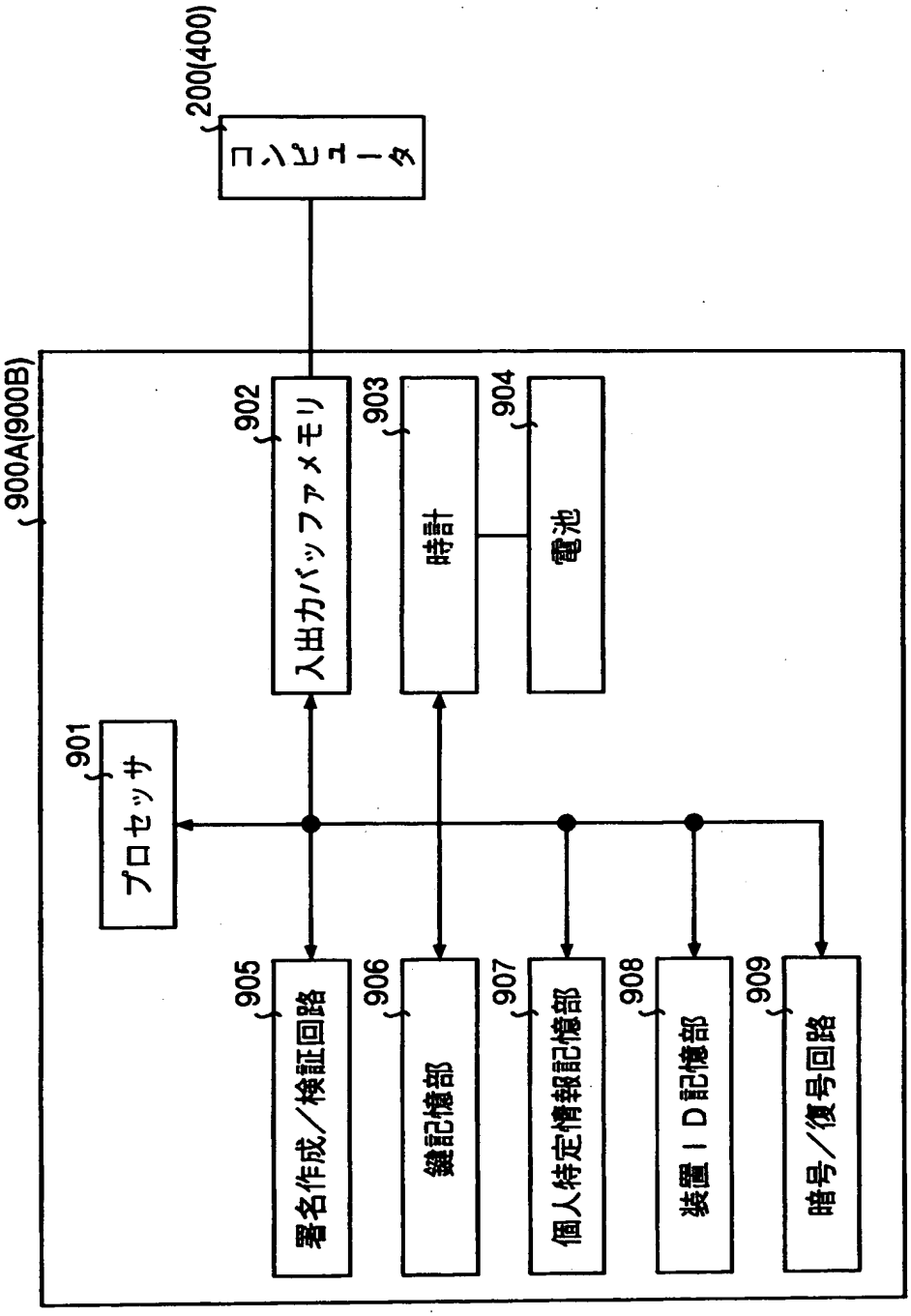
【図１１】

実施の形態３の構成を示すブロック図



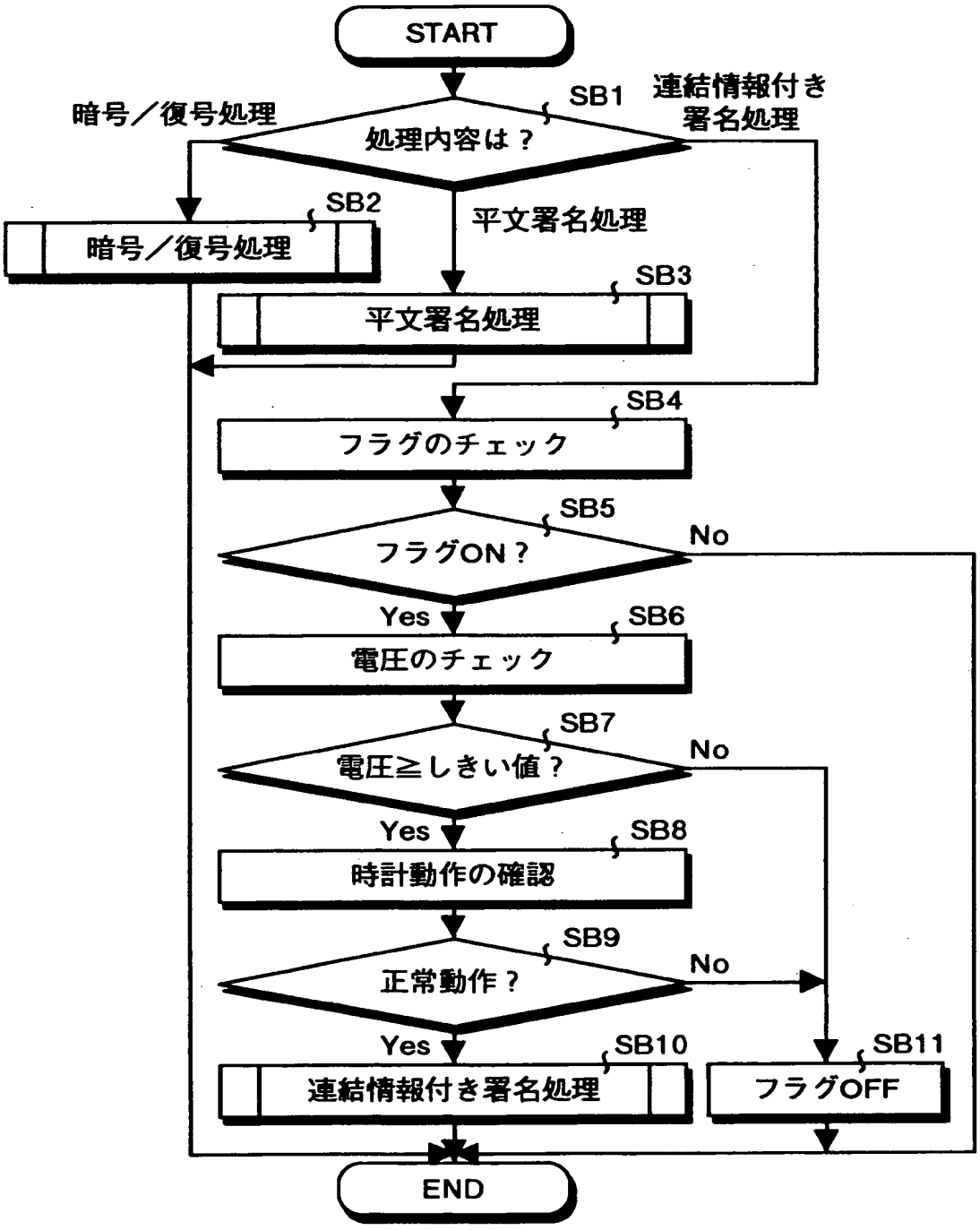
【図１２】

図11に示した署名装置900A（900B）の構成を示すブロック図



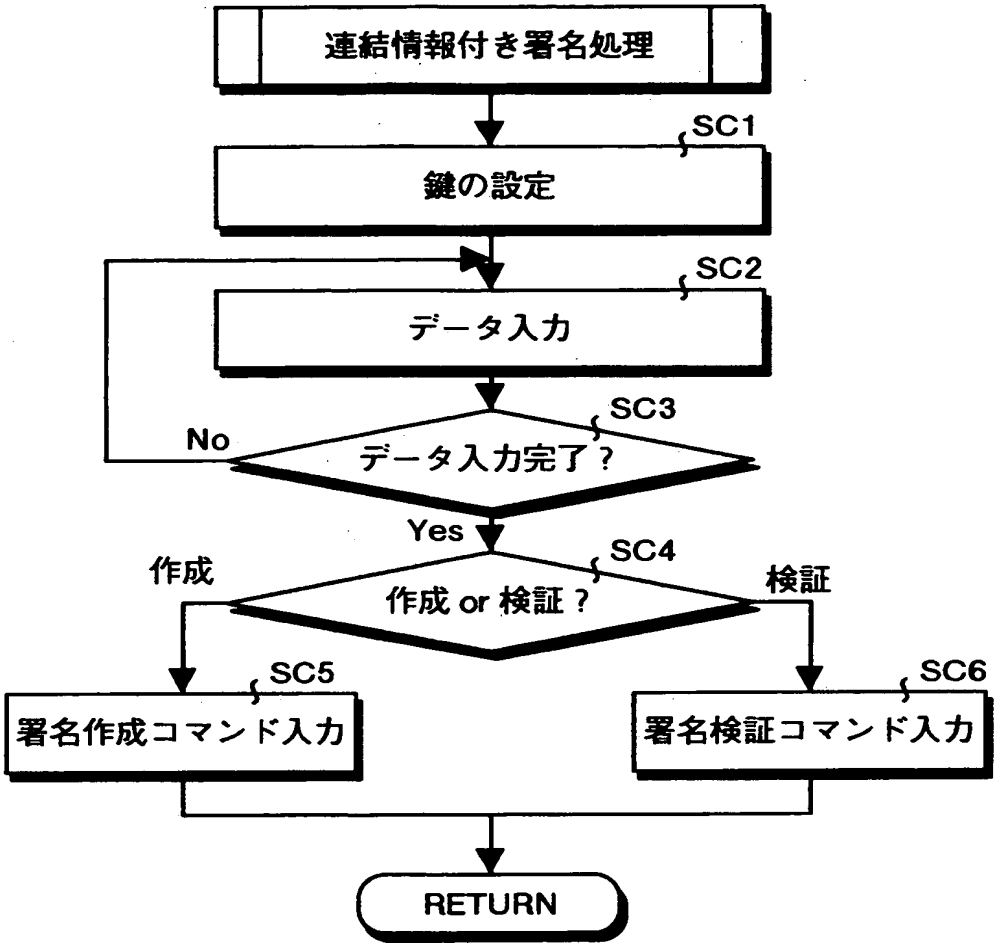
【図１３】

実施の形態３の動作を説明するフローチャート



【図１４】

実施の形態３における連結情報付き署名処理を説明するフローチャート



【書類名】　　要約書

【要約】

【課題】　日時の改竄を防止することができるとともに、ディジタル署名を行った者、装置を特定することができ、しかも作成者に関する情報の変更に柔軟に対応できる署名作成装置および署名検証装置ならびに署名装置を提供すること。

【解決手段】　ディジタル署名の作成の日時の認証に用いられる日付、時刻等の時間に関するタイムスタンプＣを生成し、ＣＡセンターに設置されたコンピュータ６００以外により時刻設定ができないようになっている時計１０３と、装置を特定するための装置ＩＤ・Ｂ、タイムスタンプＣおよび作成者を特定するための個人特定情報Ｄを平文Ａに連結することで署名対象データＥを作成する連結部１０２、１０６および１０９と、署名対象データＥを署名作成鍵K_{c1}”等で暗号化し、署名Ｌを作成する署名作成回路１１２と、署名対象データＥに署名Ｌを連結し、署名済みデータＭとして送出する連結部１１３とを備える。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社